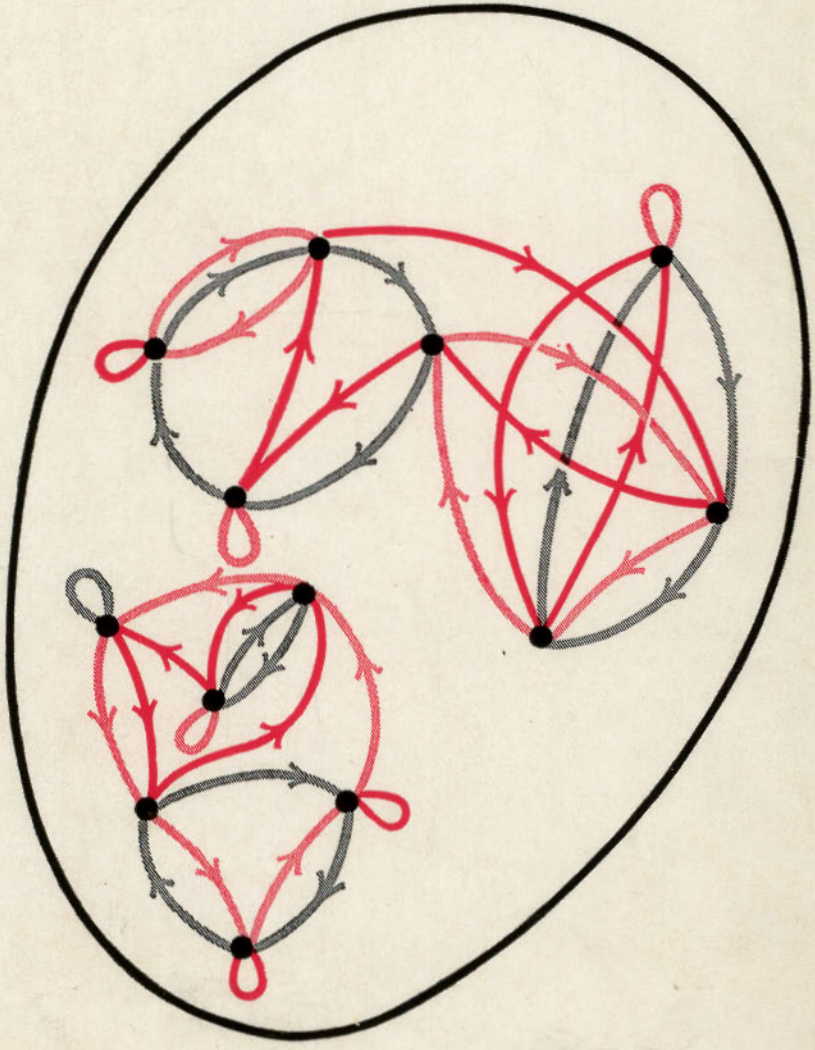
GROUPS

GEORGES PAPY



GROUPS

GEORGES PAPY

MACMILLAN

GROUPS

By Professor Georges Papy

Belgian Centre of Pedagogic Mathematics, University of Brussels

Professor Papy's book is already well known in its original French version. Now Mary Warner's translation thoroughly reflects the author's spirit in presenting a rigorous yet exciting introduction to a subject that has a central and fundamental position in modern mathematics. In this transitional period, when group theory is only just permeating teaching in schools, the book will serve to stimulate the thinking of teachers (both practising and in training) and mathematical students in Universities, C.A.T.s and Technical Colleges.

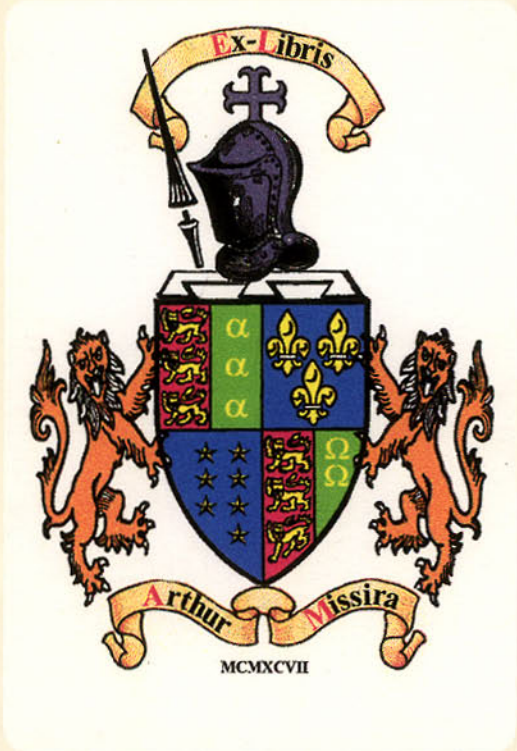
The success of this book is partly due to the inclusion of a large number of exercises which guide and help the reader as each new topic is developed, whilst 32 coloured plates help visualisation of some of the abstract arguments.

The Author

In addition to his Presidency of the *Belgian Centre of Pedagogic Mathematics*, Professor Papy is also President of the *International Commission for the Study and Improvement of the Teaching of Mathematics* and President of the *Belgian Centre of Algebra and Topology*. He has written widely on modern algebra and geometry, and has lectured extensively on these subjects throughout the world.

42s net

Groups



Groups

GEORGES PAPY

Professor at the University of Brussels

Translated by Mary Warner

LONDON
MACMILLAN & CO LTD
NEW YORK · ST MARTIN'S PRESS
1964

First Edition 1961
Presses Universitaires de Bruxelles
Dunod – Paris

First English edition 1964
Macmillan & Company Limited, London

Translated by Mary Warner

MACMILLAN AND COMPANY LIMITED
St Martin's Street London WC2
also Bombay Calcutta Madras Melbourne

THE MACMILLAN COMPANY OF CANADA LIMITED
Toronto

ST MARTIN'S PRESS INC
New York

PRINTED IN GREAT BRITAIN BY
WILLIAM CLOWES AND SONS, LIMITED, LONDON AND BECCLES

In Memoriam

GUSTAVE VERRIEST

Translators Note

The translator has added part II of the Appendix, the description of the plates, and footnotes prefaced by Tr.

Preface

Since the part played by the concept of a "group" as a fundamental element of basic mathematics is universally recognized, it is desirable that the elements of the theory of groups should be taught from the secondary school, not as a supplementary chapter, but indeed as a basic part of the structure of mathematics.

In spite of the vast movement to modernize the teaching of mathematics which is apparent throughout the world, most of our pupils leave the secondary school without having met this important mathematical concept.

Thus we see the magnitude and the urgency of the task to be done.

The aim of this book is to contribute to this indispensable reform by producing an introductory text to the fundamentals of the theory of groups.

During this transitional period, it is intended equally for secondary school teachers, for university students, for students at training colleges, and for pupils in the higher classes of secondary schools.

The author hopes that a great part of the material covered by this book will soon be integrated as basic teaching in secondary schools. For the present, it is imperative to teach the ideas of group theory without further delay.

* * *

Like all fundamental ideas, that of a "group" must be freed from the particular form in which it has been defined. That is why Chapter 1 gives, as close together as possible, two equivalent definitions of groups and insists on the properties of the neuter and the symmetric of every element.

Chapter 2 illustrates the idea of a group with examples and counter-examples, both equally important.

Chapter 3 is especially useful in its applications to secondary school teaching and can clarify problems involving negative and fractional exponents as well as the roots of unity.

In the first three chapters the actors are the groups and their elements. In Chapter 4 the theory moves to another plane by considering privileged subsets, stable subsets and subgroups. Experience shows that the study of subsets of known groups provides situations of great interest to the pupils.

Chapter 5 reviews some supplementary results on commutative groups.

In Chapter 6 we have sought to show how the use of group theory ideas animates and enriches the teaching of elementary arithmetic and leads quite naturally to the concepts of a ring and a lattice. The teaching of arithmetic along these lines is at the same time an excellent exercise for mastering group theory. The methods used are fundamental and may be applied time and again in further studies.

Chapter 7 shows the important relations which can exist between different groups. In particular it discusses the homomorphism and isomorphism theorems which are fundamental in present-day mathematics.

Chapter 8 is devoted to the specific study of permutations of sets, finite or otherwise.

In Chapter 9 the introduction of the concept of a group with operators considerably extends the scope of the theory. With its help, the theory of vector spaces and that of ideals become attached directly to the common stem of group theory.

The last chapter is devoted to the concept of dimension in the theory of groups with operators. The theorems of Jordan-Hölder, Schreier and Zassenhaus will be found there. We know that this theory for groups with operators is essentially due to Emmy Noether and Krull.

The text of the book assumes that the reader will do all the exercises which appear in the main body of the chapters. Even this is not enough. The reader will become thoroughly familiar with the many-sidedness of the theory of groups only by himself searching in his personal mathematical equipment for illustrations of the properties studied.

The revision exercises should allow the reader to check his attainments in group theory. They are sometimes used to introduce new ideas, very important in algebra, but whose systematic exposition is outside the scope of this book.

* * *

In the appendix there will be found a résumé of the main definitions and notations of set theory used in this book. We strongly advise that resort should be made to them only when necessary.

* * *

The coloured plates illustrate the theory more than the text itself. They present situations of a kind to inspire the reader and to increase his understanding. They suggest methods for the elementary teaching of the fundamentals of group theory.

* * *

I thank Frédérique Papy for the strict discipline which she has imposed on me, and without whom this work would never have seen the light of day. I am indebted to her, moreover, for a valuable pedagogic experience.

I wish to express my gratitude to M. Roger Holvoet, Assistant at the University, for his judicious observations and for the substantial lists of revision exercises which he kindly prepared.

The reader is indebted to Monsieur Pierre Debbant, Assistant at the Belgian centre for Algebra and Topology, for the index which appears at the end of the book, and for a large number of improvements in the text.

I thank especially Monsieur Henri Levarlet, Director-general of Secondary and "Normal" Teaching, and Monsieur Jean Van Hercke, Secretary-general to the Reform of Secondary teaching, for the considerable support which they have never stopped giving us in this enterprise of reforming the teaching of mathematics.

Brussels, June 13th 1961 GEORGES PAPY

Preface to English Edition

During the last few years I have had the privilege of talking quite frequently to fellow mathematicians and teachers in England. The reception they have given me has been such that I feel truly at home in this country in which the concern for good teaching is most impressive.

I also feel it is to friends that I am today presenting this book which is the fruit of a sincere effort to improve the teaching of mathematics.

I should like to thank all those who have received me so kindly and in particular Professor K. A. Hirsh and Miss Hazel Perfect who have made the translation of this work possible. I should like to express my gratitude to the translator Mrs. Mary Warner who has accomplished her task to perfection. The notes that she has added constitute a real improvement on the original text. Finally I thank the house of Macmillan which with its accustomed care has carried through the publication of this book.

GEORGES PAPY

Contents

Page

CHAPTER 1

DEFINITION AND FUNDAMENTAL PROPERTIES OF GROUPS

Section

1 Introduction 1
2 Definition of a group 3
3 Fundamental properties of groups 3
4 A new definition of a group 8
5 Inverse laws in G, $*$ 9
6 Commutativity 10
7 The symmetric of a product 10
8 Cancellation 11

CHAPTER 2

SUPPLEMENTARY COMMENTS—
ILLUSTRATIONS OF THE IDEA OF A GROUP

1 Equality 12
2 Additive and multiplicative groups 12
3 Standard notations 13
4 Examples of laws which are not laws of groups 14
5 Examples of groups 16
6 General associativity 20
Revision exercises on Chapters 1 and 2 22

CHAPTER 3

THE SCALAR LAW OF A GROUP

1 Introduction 30
2 The outer law: $\omega_0 \times G \to G$ 30
3 The scalar law of the group G, $*$ 31
4 Properties of the scalar law 31

Contents

Section		Page
5	Supplementary properties of the scalar law in the case of a commutative group G, $*$	31
6	The scalar law in a group G,.	32
7	The scalar law of a group G, +	33
8	The scalar law in the symmetric group $\mathscr{S}$E, $\circ$ of the set E	33
9	Mixed associativity	34
10	Exercises	34
11	Divisible groups	35

CHAPTER 4

SUBGROUPS

1	Example	38
2	Stable subsets and subgroups	38
3	The neutral element and the symmetric in a subgroup	40
4	A new characterization of subgroups	40
5	Trivial subgroups	41
6	The intersection of a set of subgroups	42
7	The subgroup generated by a subset of a group	42
8	Moore's closure	43
9	Generating subsets	44
10	Cyclic groups	44
11	Exercises	45
12	An expression for the subgroup generated by a subset of a group	46
13	Cosets, the order of a group and of a subgroup	47
14	Exercises	50
Revision exercises on Chapter 4		51

CHAPTER 5

MODULES OR COMMUTATIVE GROUPS

1	Intersection of submodules	55
2	Product of subgroups of a group G, $*$	55
3	Addition of submodules	56

Contents

Section		Page
4	Lattices	57
5	Exercise	58
6	Dedekind's theorem	58
Revision exercises on Chapter 5		61

CHAPTER 6

THE GROUP Z, +

1	Introduction	62
2	Fundamental properties of Z, +, $\leqslant$	62
3	Definition of multiplication in Z, +	64
4	The ordered ring Z, +, ., $\leqslant$	66
5	Study of Z, .. Factorization	67
6	The Euclidean ring Z, +, ., $\leqslant$	70
7	The submodules of Z, +	72
8	The structures Z, $\wedge$, $\vee$ and ω, $\wedge$, $\vee$	73
9	The factorial ring Z, +, .	75
10	Factorization in ω	77
11	Sets of divisors and filtering sets	80
12	The distributive lattice ω, $\wedge$, $\vee$	83
13	Utilization of the properties of Z, + in the study of groups	83
Revision exercises on Chapter 6		86

CHAPTER 7

HOMOMORPHISMS AND QUOTIENT GROUPS

1	The group R, + and plane rotations	90
2	Homomorphism	90
3	Examples and exercises	91
4	The image of a homomorphism	94
5	A reminder of some set-theory notations	96
6	The quotient of a homomorphism	97
7	The homomorphism theorem	98
8	The law induced on the set of subsets of a group	99
9	Study of G/h	100
10	The quotient of a group by a normal subgroup	104

Contents

Section		*Page*
11	First isomorphism theorem (Emmy Noether)	106
12	Second isomorphism theorem	107
Revision exercises on Chapter 7		109

CHAPTER 8

PERMUTATIONS

1	Definition (revision)	125
2	Minimal permutations	127
3	Partition of a permutation into minimal permutations	128
4	Finite permutations and cycles	134
5	Decomposition of a permutation of a finite set into cycles	137
6	Decomposition of finite permutations into the product of transpositions	140
7	The alternating group	143
Revision exercises on Chapter 8		145

CHAPTER 9

GROUPS WITH OPERATORS

1	A unifying concept	150
2	Examples	150
3	Groups with operators	152
4	Exercises	152
5	Admissible subgroups	157
6	Theorem	158
7	Exercises	158
8	The quotient by an admissible normal subgroup	160
9	The image and kernel of an admissible homomorphism	161
10	Homomorphism theorem for groups with operators	163
11	Isomorphism theorems	166
Revision exercises on Chapter 9		167

Contents

Section		*Page*

CHAPTER 10

DIMENSION

1	The vector space of ordinary space	171
2	Normal chains	172
3	Proof of the Jordan–Hölder theorem	176
4	Schreier's theorem	178
Revision exercises on Chapter 10		191
REVISION EXERCISES ON THE BOOK		195
APPENDIX		211
TRANSLATOR'S APPENDIX		212
TERMINOLOGICAL INDEX		215
LIST OF PLATES		219

1

Definition and Fundamental Properties of Groups

§1. INTRODUCTION

From the most elementary level mathematics makes systematic use of operations or (binary) laws. Addition, multiplication, subtraction and division of whole numbers are laws. A law associates with certain pairs (of elements) an element called the result. For example, subtraction associates the number 2 with the pair (5, 3). We note this fact by writing $\boxed{5 - 3 = 2}$. Thus $5 - 3$ is the result of the law $-$ applied to the pair (5, 3).

In general, we denote by $a * b$ the result of the law $*$ applied to the pair (a, b).

A law is said to be inner and everywhere defined in E if and only if it assigns to every pair of elements of E a result belonging to the set E.

In other words, an inner law everywhere defined in the set E is a mapping of $E \times E$ into E.

More formally, we can say:

The law $*$ is inner and everywhere defined in E if and only if

$$\forall x, y \in E: \qquad x * y \in E$$

If the law $*$ is an inner law everywhere defined in E, we say that the set E is provided with the law $*$, and we call E, $*$ an algebraic structure.

It is easy to give numerous examples of laws.

The H.C.F. and L.C.M. of positive integers define inner laws in the set ω of positive integers. Intersection, union and difference define inner laws in the set $\mathscr{P}E$ of subsets of the set E.†

Two distinct points of ordinary space define a straight line. We are dealing here with a law defined only for distinct pairs of points; the result of the operation is a straight line: the law is thus neither inner nor everywhere defined.

† Tr. See Appendix.

The foregoing examples, many more of which could have been cited, demonstrate the importance of the concept of a law in the most diverse branches of mathematics.

This justifies the elaboration of a general theory.

In particular, we shall study groups, i.e. sets provided with a law satisfying special conditions. We shall see that Z, + ; R, + ;† $\mathscr{P}$E, $\triangle$ where $\triangle$ denotes the symmetric difference‡; and the set of permutations of a set§ (provided with the product of composition) are all examples of groups.

Before giving the precise definition of a group, let us note two properties common to the structures just considered.

(a) We may always pass from a (binary) law involving two terms to an operation involving several terms. Thus,

$$2 \times 3 \times 7 = (2 \times 3) \times 7$$
$$2 - 3 - 7 = (2 - 3) - 7$$

In the first case, we have

$$(2 \times 3) \times 7 = 2 \times (3 \times 7)$$

which is not so in the second case, since

$$(2 - 3) - 7 \neq 2 - (3 - 7)$$

We shall say that the law $\times$ is associative while the law $-$ is not.

Associativity. We shall say that the inner law $*$ everywhere defined in the set E is associative if and only if

$$(a * b) * c = a * (b * c)$$

for all choices of elements a, b, c (distinct or otherwise) of the set E. The laws of the structures considered above are all associative.

(b) If a and b are rational integers† there exist rational integers x and y such that

$$a + x = b = y + a$$

(We even have $x = y$ as a consequence of the commutativity of $+$.)

The same property holds in R, +.

If f and g are permutations‡ of E, there always exist permutations p and q of E such that

$$f \circ p = g = q \circ f$$

† Tr. See Ch. 2, §3. ‡ Tr. See Appendix. § Tr. See Ch. 2, §5 (g).

This property, together with associativity, characterizes completely the law of a group.

§2. DEFINITION OF A GROUP

Definition. A group is defined as any non-empty set G *provided with an inner law everywhere defined and associative and such that*

$$\forall a, b \in G, \exists x, y \in G: \qquad a * x = b = y * a \tag{1}$$

We denote by

$$G, *$$

the group formed by the set G provided with the law $*$. When there is no fear of confusion, we sometimes write G instead of G, $*$

Note: Since the law $*$ of the group G, $*$ is inner and everywhere defined:

$$\forall a, b \in G: \qquad a * b \in G$$

The associativity of $*$ implies

$$\forall a, b, c \in G: \qquad (a * b) * c = a * (b * c)$$

The reader should verify that the structures described at the beginning of this paragraph are indeed groups.

In the case of $\mathscr{P}$E, $\triangle$ note that if A, B $\in \mathscr{P}$E, then

$$A \triangle (A \triangle B) = B = (B \triangle A) \triangle A$$

§3. FUNDAMENTAL PROPERTIES OF GROUPS

(a) *Existence and uniqueness of the neuter*†

Let us consider a group G, $*$. (Therefore $G \neq \varnothing$)‡. Let $g \in G$.

From the definition of a group it follows that there exists (at least) one element $n \in G$ such that

$$g * n = g \tag{1}$$

We shall show that

$$\forall h \in G: \qquad h * n = h \tag{2}$$

The definition of a group guarantees the existence of a $k \in G$ such that

$$h = k * g \tag{3}$$

† Tr. This is sometimes called the unity or unit element.
‡ Tr. See Appendix.

From this we obtain successively

$$\begin{aligned} h * n &= (k * g) * n && \text{(by (3))} \\ &= k * (g * n) && \text{(associativity of } *) \\ &= k * g && \text{(by (1))} \\ &= h && \text{(by (3))} \end{aligned}$$

Thus

$$h * n = h$$

Q.E.D.

Similarly we could have proved the existence of a left neutral element, i.e. an element $m \in \mathrm{G}$ such that

$$\forall g \in \mathrm{G}: \qquad m * g = g$$

We have just shown that the set M of left neuters and the set N of right neuters are non-empty. Let $w \in \mathrm{M}$ and $v \in \mathrm{N}$ and let us consider the expression $w * v$.

Then

$$w * v = w$$

since v is a right neuter, and

$$w * v = v$$

since w is a left neuter.

Thus,

$$w = w * v = v$$

hence

$$w = v$$

The last equality shows that every left neuter is equal to every right neuter. It follows that all left neuters are equal and that they are also equal to all right neuters. We have therefore proved that in the group G, $*$ there exists a special element ν which is at the same time the only left neuter and the only right neuter of the group.

The neutral element ν of the group G, $*$ is thus characterized by the property

$$\forall g \in \mathrm{G}: \qquad \nu * g = g = g * \nu$$

Let us recapitulate the main results and definitions we have just met.

Definitions. Let E *be a non-empty set provided with an inner law everywhere defined and written* $*$. *Every element* n *of* E *such that* $x * n = x$ *for every* $x \in \mathrm{E}$ *is called a right neuter for the law* $*$.

Every element m *of* E *such that* $m * x = x$ *for every* $x \in \mathrm{E}$ *is called a left neuter for the law* $*$.

Every element ν *of* E *which is simultaneously a right neuter and a left neuter, i.e. such that* $\nu * x = x = x * \nu$ *for every* $x \in \mathrm{E}$, *is called a neutral element for the law* $*$.

Proposition 1. Every group contains a unique neutral element which is moreover the unique left neuter and the unique right neuter of the group.

(b) *Existence and uniqueness of the symmetric*† *of every element of a group*

From the definition of a group we know that G is non-empty. We now know that G contains a particular element: the neuter ν. Let us make ν play the part of the element b in the definition of a group (see §2).

From this definition, for every $a \in \mathrm{G}$, there exist elements a' and a'' such that

$$a * a' = \nu = a'' * a \tag{4}$$

Then we have successively

$$\begin{aligned} a'' &= a'' * \nu && \text{(since } \nu \text{ is the neuter of the group)} \\ &= a'' * (a * a') && \text{(first equation of (4))} \\ &= (a'' * a) * a' && \text{(associativity of } *) \\ &= \nu * a' && \text{(second equation of (4))} \\ &= a' && \text{(neuter of the group)} \end{aligned}$$

From which it follows that

$$a' = a''$$

We describe $a * a' = \nu$ by saying that a' is a right symmetric of a. Similarly, a'' is a left symmetric of a. The relation $a' = a''$ is valid for every right symmetric a' and for every left symmetric a'' of a. All the left symmetrics are therefore equal to any one right symmetric. It follows that all the left symmetrics are equal and that they are also equal to all the right symmetrics.

In other words, every element of a group has one and only one

† Tr. Sometimes called the inverse of an element.

left symmetric and one and only one right symmetric and these elements are equal.

Let us recapitulate below the main propositions and definitions which we have just met.

Definitions. *Let* $G, *$ *be a group whose neuter is given by* ν. *Given* $g \in G$, *every* $g' \in G$ *such that* $g * g' = \nu$ *is called a left symmetric of* g. *Every* $g'' \in G$ *such that* $g'' * g = \nu$ *is called a right symmetric of* g. *Every element of* G *which is simultaneously a left symmetric and a right symmetric of* g *is called a symmetric of* g.

Proposition 2. *In a group every element* g *admits a unique symmetric which is moreover the only left symmetric and the only right symmetric of this element.*

Notation. In the group $G, *$ we denote by $\bar{a}$ the symmetric of a.

(c) *Solution of equations in a group* $G, *$

The definition of a group states that whatever the elements $a, b \in G$, the equations

$$a * x = b$$
$$y * a = b$$

have solutions in G.

Let us calculate them:

The first of these equations implies

$$\bar{a} * (a * x) = \bar{a} * b$$

Hence, by associativity,

$$(\bar{a} * a) * x = \bar{a} * b$$

and since $\bar{a} * a = \nu$, we get

$$\nu * x = \bar{a} * b$$

and finally

$$x = \bar{a} * b$$

Similarly we could establish that

$$y = b * \bar{a}$$

The definition of a group tells us that each of the equations

$$a * x = b \qquad y * a = b$$

has at least one solution. We now know that these solutions are unique since the given equations imply that

$$x = \bar{a} * b \quad \text{and} \quad y = b * \bar{a}$$

Thus we have proved the uniqueness of the solutions x and y to the equations

$$a * x = b = y * a$$

Proposition 3. *In a group* $G, *$, *for every choice of elements* $a, b \in G$, *there exists one and only one element* $x \in G$ *and one and only one element* $y \in G$ *such that*

$$a * x = b = y * a$$

The solution (x, y) is given by $x = \bar{a} * b$, $y = b * \bar{a}$.

(d) *New characterization of the neuter*

The neutral element ν of the group $G, *$ obviously satisfies the relation

$$\nu * \nu = \nu$$

Let x be an element of G satisfying

$$x * x = x \tag{5}$$

We shall prove that (5) implies $x = \nu$.

Equation (5) implies that

$$\bar{x} * (x * x) = \bar{x} * x$$

and it follows as a consequence of associativity that

$$(\bar{x} * x) * x = \bar{x} * x$$

and since $\bar{x} * x = \nu$, then

$$\nu * x = \nu$$

and finally

$$x = \nu$$

Q.E.D.

Definition. *Let* $E, *$ *be a set provided with the law* $*$ *everywhere defined. An element* e *of* E *is called an idempotent if and only if we have*

$$e * e = e$$

Proposition 4. *The neuter of a group is its only idempotent.*

§4. A NEW DEFINITION OF A GROUP

Every group contains a neuter and every element of a group has a symmetric.

We shall show that these properties together with associativity characterize groups (thus giving a new definition).

Proposition 5. Let G *be a set provided with an inner law* $*$, *everywhere defined, associative and possessing a neutral element* ν. *If in addition, every element of* G *possesses a symmetric in* G, *then* G, $*$ *is a group.*

We must prove that for every $a, b \in G$, there exist $x, y \in G$ such that

$$a * x = b = y * a \tag{1}$$

The hypothesis tells us that a possesses (at least) one symmetric. Let a' be a symmetric of a.

We shall show that the elements $x = a' * b$ and $y = b * a'$ of G satisfy equations (1).

In fact,

$$\begin{aligned} a * x &= a * (a' * b) && \text{(definition of } x\text{)} \\ &= (a * a') * b && \text{(associativity of } *\text{)} \\ &= \nu * b && \text{(property of the symmetric of an element)} \\ &= b && \text{(neuter of the group)} \end{aligned}$$

Similarly

$$\begin{aligned} y * a &= (b * a') * a && \text{(definition of } y\text{)} \\ &= b * (a' * a) && \text{(associativity of } *\text{)} \\ &= b * \nu && \text{(symmetric of an element)} \\ &= b && \text{(neuter of the group)} \end{aligned}$$

Q.E.D.

Proposition 5 gives us a new definition of a group.

Definition. Every set G, $*$ *provided with an inner law, everywhere defined, associative, possessing a neutral element, and such that every element* $g \in G$ *has a symmetric belonging to* G *is called a group.*

This definition, like the first, confines itself to stipulating the existence of certain elements: a neuter, and a symmetric for every element. We know that this implies the uniqueness of the neuter and the uniqueness of the symmetric.

Proposition 6. In the group G, $*$ *every element is the symmetric of its symmetric.*

In other words:

$$\forall g \in G: \qquad \bar{\bar{g}} = g$$

Proof

It is sufficient to note that the formula

$$a * b = \nu = b * a$$

expresses at the same time that b is the symmetric of a and that a is the symmetric of b.

§5. INVERSE LAWS IN G, $*$

We know that for every pair (u, v) of elements of G the equation

$$x * v = u$$

has in G the unique solution given by

$$x = u * \bar{v}$$

Thus, with every pair (u, v) of elements of G let us associate the element $u * \bar{v}$ of G, thereby defining an inner law in G, $*$

$$u \mathbin{\overline{*}} v = u * \bar{v}$$

(In more detail: $G \times G \to G$: $(u, v) \to u \mathbin{\overline{*}} v = u * \bar{v}$.)

Similarly, the equation $v * x = u$ has the unique solution $x = \bar{v} * u$, thus defining the inner law

$$u \mathbin{\underline{*}} v = \bar{v} * u$$

We shall say that the laws $\overline{*}$ and $\underline{*}$ are the inverse laws of G, $*$. To distinguish them, we shall say that $\overline{*}$ is the right inverse law and $\underline{*}$ is the left inverse law.

Nevertheless, simply for the sake of brevity, we shall frequently refer to $\overline{*}$ as the inverse law of G, $*$.

Exercises

1. In general, the law $\overline{*}$ is neither associative nor commutative. The element ν is a right neuter for this law since $x \mathbin{\overline{*}} \nu = x * \nu = x$ for every $x \in G$. This law does not in general possess a left neuter.

2. In general it is not true that

$$y \mathbin{\underline{*}} x = x \mathbin{\overline{*}} y$$

Prove the formulae

$$\overline{x \bar{*} y} = y \bar{*} x$$

and

$$\overline{x \underline{*} y} = \bar{x} \bar{*} \bar{y}$$

3. In a group G, $*$ we have

$$x \bar{*} \bar{y} = x * y$$

4. In a group $\bar{\nu} = \nu$. Show that this property does not always characterize the neuter ν.

§6. COMMUTATIVITY

If a and b are elements of the group G, $*$, we do not always have $a * b = b * a$.

If in a group M, $*$ we have

$$\forall x, y \in \mathrm{M}: \qquad x * y = y * x$$

we say that the group M, $*$ is commutative (we also say that the law $*$ is commutative).

Examples

The groups R, +; R_0, .† are commutative. The symmetric group‡ of a set consisting of at least three distinct elements is not commutative.

More generally, we shall say that *a law $*$ is commutative* if and only if $x * y = y * x$ for all pairs (x, y) for which the law is defined.

§7. THE SYMMETRIC OF A PRODUCT

If a and b are elements of the group G, $*$, then so is $a * b$. This last element therefore has a symmetric $\overline{a * b}$ which we shall find.

Proposition 7. *In a group* G, $*$

$$\forall a, b \in \mathrm{G}; \qquad \overline{a * b} = \bar{b} * \bar{a}$$

Proof

Since the symmetric of an element is the sole right symmetric, it is sufficient to show that

$$(a * b) * (\bar{b} * \bar{a}) = \nu$$

† Tr. See Ch. 2, §3. ‡ Tr. See Ch. 2, §5 (g).

By associativity we can write

$$(a * b) * (\bar{b} * \bar{a}) = ((a * b) * \bar{b}) * \bar{a}$$

In fact, putting

$$a * b = c \tag{2}$$

we have

$$\begin{aligned} (a * b) * (\bar{b} * \bar{a}) &= c * (\bar{b} * \bar{a}) && \text{(by (2))} \\ &= (c * \bar{b}) * \bar{a} && \text{(associativity of } *) \\ &= ((a * b) * \bar{b}) * \bar{a} && \text{(by (2))} \end{aligned}$$

From this we obtain successively:

$$\begin{aligned} ((a * b) * \bar{b}) * \bar{a} &= (a * (b * \bar{b})) * \bar{a} && \text{(associativity of } *) \\ &= (a * \nu) * \bar{a} && (b * \bar{b} = \nu) \\ &= a * \bar{a} && (a * \nu = a) \\ &= \nu && \text{(symmetric of an element)} \end{aligned}$$

Q.E.D.

§8. CANCELLATION

In elementary algebra we learn to simplify a fraction by dividing each of its terms by the same number, and a little later on we sometimes say that we simplify an equation by adding or subtracting the same term to or from each side. In both these cases we are in fact applying the property of cancellation of groups.

Proposition 8. *If a, b, c are elements of a group* G, $*$, *then the equation* $a * b = a * c$ (1) *implies* $b = c$. *Similarly, the equation* $a * c = b * c$ (2) *implies* $a = b$.

Proof

We confine ourselves to proving the first part of the theorem.

Equation (1) implies

$$\bar{a} * (a * b) = \bar{a} * (a * c)$$

From this, by associativity

$$(\bar{a} * a) * b = (\bar{a} * a) * c$$

Remembering that $\bar{a} * a = \nu$, we have

$$\nu * b = \nu * c$$

and finally

$$b = c$$

Q.E.D.

2

Supplementary Comments—Illustrations of the Idea of a Group

§1. EQUALITY

We have several times used the equality sign $=$ without explanation. Perhaps it would be of some use here to recall its meaning.

When we write $(a * b) * c = a * (b * c)$ we simply wish to indicate that the collections of terms $(a * b) * c$ and $a * (b * c)$ denote the same element (or object). We shall keep as strictly as possible to this point of view. However we record that common practice in English-speaking countries sometimes deviates regrettably from this. Such would be the case if we described as equal two triangles which were different but superimposable.

§2. ADDITIVE AND MULTIPLICATIVE GROUPS

We often use the sign $+$ or the sign $\cdot$ to denote the law of a group. A law whose sign is $+$ is called addition and a group whose law is written $+$ is sometimes referred to briefly as an *additive group*. The neutral element of an additive group is almost always written 0 and is then called zero. The symmetric of the element x of an additive group is written $-x$ and is called the negative of the element x. We then have $-(-x) = x$ and $-(x + y) = (-y) + (-x)$. The (right) inverse law of an additive group is called subtraction and is written $-$.

Thus

$$x - y = x + (-y)$$

and

$$-(x + y) = -y - x$$

Some authors keep the sign $+$ for commutative laws.

A law written . is often called multiplication. The result of a multiplication is called the product. A group whose law is written . is often referred to briefly as a *multiplicative group*. The neutral element of a multiplicative group is called the unity or identity, and is

usually represented by a symbol such as 1, I, ϵ, etc. In a multiplicative group the symmetric of an element x is called its inverse and is written x^{-1}. We then have $(x^{-1})^{-1} = x$ and $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$. The (right) inverse law of a multiplicative group is called division, or better still, right division. In the case of a commutative group, the inverse law is written /.

Thus

$$x/y = x \cdot y^{-1}$$

and

$$(x/y)^{-1} = y/x$$

Exercise

In a group G, $+$ we have

$$x - y = x + (-y)$$

and

$$x - (-y) = x + y$$

In a commutative group G, $\cdot$ we have

$$x/y = x \cdot y^{-1}; \qquad x/y^{-1} = x \cdot y;$$
$$x/y = y^{-1}/x^{-1}$$
$$(x/y)^{-1} = y/x$$
$$x^{-1} = 1/x$$

§3. STANDARD NOTATIONS

We shall always denote:

by ω the set of natural integers,
(natural numbers)
by Z the set of rational integers,
by Q the set of rational numbers,
by R the set of real numbers,
and by C the set of complex numbers.

We shall denote by ω_0 the set ω without the element 0, and we shall define in the same way Z_0, Q_0, R_0, and C_0.

We then have

$$\omega = \{0, 1, 2, 3, \ldots\}$$
$$\omega_0 = \omega \setminus \{0\} = \{1, 2, 3, \ldots\}\dagger$$
$$Z = \{0, 1, -1, 2, -2, \ldots\}$$

† Tr. See Appendix.

$$\begin{aligned} Z_0 &= Z \setminus \{0\} = \{1, -1, 2, -2, \ldots\} \\ Q &= \{a/b \mid a \in Z, b \in \omega_0\}\dagger \\ Q_0 &= Q \setminus \{0\} \\ &= \{a/b \mid a \in Z_0, b \in \omega_0\} \\ R_0 &= R \setminus \{0\} \\ C &= \{a + bi \mid a, b \in R\} \\ C_0 &= C \setminus \{0\} \end{aligned}$$

We shall denote by R^+ the set of positive real numbers, and by R^- the set of negative real numbers. Quite naturally, R_0^+ denotes the set of strictly positive reals, and R_0^- the set of strictly negative reals. For every subset P of R, we shall write

$$P^+ = P \cap R^+\dagger$$

and

$$P_0^+ = P \cap R_0^+$$

We then have

$$\begin{aligned} Q_0^- &= \{-a/b \mid a, b \in \omega_0\} \\ Z^+ &= \omega \\ Z^- &= -\omega = \{-n \mid n \in \omega\} \end{aligned}$$

§4. EXAMPLES OF LAWS WHICH ARE NOT LAWS OF GROUPS

We shall better understand the concept of a group by examining laws which do not satisfy all the conditions required of the laws of groups.

(a) Addition in ω is an inner law, everywhere defined, associative, (and commutative); it admits a neutral element, and the cancellation rule holds. However, it is not a law of a group. To see this, it is sufficient to note that the equation $87 + x = 49$ does not possess a solution in ω.

(b) Subtraction in Z is a law which is everywhere defined but not associative. This law is not commutative; it admits a right neuter but not a left neuter.

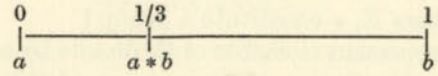
(c) Multiplication in ω is a law everywhere defined and associative, but it is not a law of a group. Why?

(d) Exponentiation in ω_0, i.e. the law defined by $a * b = a^b$, is an inner law, everywhere defined; it is not associative. (How would you prove this?) This law is not commutative. It admits a right neuter but not a left neuter. (What is this right neuter?)

† Tr. See Appendix.

(e) If a and b represent points of ordinary space E, let us denote by $a * b$ the middle of the segment $[ab]$. In particular $a * a = a$ for every point of the space. Can you deduce that E, $*$ is not a group? (Justify your reply in detail.) Is the law $*$ associative? Does it admit a neuter?

(f) If a and b represent points of ordinary space E, denote by $a * b$ the point of the segment $[ab]$ which divides this segment in the proportion 1/3.



How can we show very quickly that E, $*$ is not a group?

(g) The set $\mathscr{P}E$ of subsets of the non-empty set E, provided with intersection, is not a group: In fact we have $P \cap P = P$ for every subset P of E.

Why did we have to assume $E \neq \varnothing$?

(h) Let E be any set. Show that $\mathscr{P}E, \cup\dagger$ is a group if and only if $E = \varnothing$.

(i) Show that $\mathscr{P}E, \setminus$ is not a group when $E \neq \varnothing$.

(j) If a and b denote natural numbers, we denote by $a \wedge b$ the H.C.F. of a and b. Show quickly that $\omega, \wedge$ is not a group.

Do the same for the law L.C.M. which we write $\vee$.

We note that the laws $\wedge$ and $\vee$ are inner laws, everywhere defined, associative and commutative. Moreover, each of these laws admits a neutral element. The reader is asked to find these neutral elements.

(k) Denote by Π a plane considered as a set of points. Let $\mathscr{D}$ be the set of straight lines in Π. If a and b are distinct non-parallel straight lines belonging to $\mathscr{D}$, we denote by $a * b$ their point of intersection. The law thus defined in $\mathscr{D}$ is commutative; it is not inner nor is it everywhere defined.

(l) With the notation of the previous example, let us put $E = \Pi \cup \mathscr{D}$. We define a law $*$ which generalizes the law $*$ which we met in (k).

If a and b denote distinct non-parallel straight lines, we continue to represent their point of intersection by $a * b$. Furthermore, for every $d \in \mathscr{D}$ we put $d * d = d$.

† Tr. See Appendix.

If $x, y \in \mathscr{D}$ and $x \parallel y$,† we denote by $x * y$ the line parallel to x and y "situated at equal distances" from x and from y.

If $p \in \Pi$, we put $p * p = p$.

If $u, v \in \Pi$ and $u \neq v$, we denote by $u * v$ the straight line which includes the points u and v.

Finally, if $p \in \Pi$ and $d \in \mathscr{D}$ we denote by $p * d$ the perpendicular to d which contains the point p.

Is the law $*$ everywhere defined in E? Is it an inner law? Is it commutative? Is it associative? Does it admit a neutral element?

Does the structure E, $*$ constitute a group?

(m) If a and b represent elements of R, denote by $a * b$ the smaller of the numbers a, b. Give a short account of the structure R, $*$. State in particular whether this law admits a neuter.

(n) Give other examples of inner laws which are not laws of groups.

§5. EXAMPLES OF GROUPS

(a) We leave to the reader the task of establishing that the following structures are groups:

$Z, +$ $\quad$ $R_0, .$
$Q_0, .$ $\quad$ $R_0^+, .$
$Q_0^+, .$ $\quad$ $C, +$
$Q, +$ $\quad$ $C_0, .$
$R, +$

(b) Denote the set of even rational integers by 2Z.

$$2Z = \{2z \mid z \in Z\}$$

Similarly, put

$$3Z = \{3z \mid z \in Z\}$$

and, more generally, for every $n \in \omega_0$,

$$nZ = \{nz \mid z \in Z\}$$

Every rational integer gives rise to a commutative group $nZ, +$.

(c) The set of complex numbers of modulus 1 is a group for multiplication.

(d) We denote by R/Z, + the structure obtained from R, + by removing the integral part of every real number. Since every real

† Tr. $x \parallel y$ means "x is parallel to y".

number may be represented as a "non-terminating decimal", the elements of R/Z may be represented by non-terminating decimals "decapitated" of their integral part. Thus

$\cdot 234792347923479\ldots$
$\cdot 14159\ldots$
$\cdot 11111\ldots$
$\cdot 00000\ldots$
$\cdot 00100000\ldots$
$\cdot 497312914853\ldots$

are elements of R/Z. Addition in R/Z is natural addition ignoring integral parts. Thus,

$$\cdot 1111\ldots + \cdot 2222\ldots = \cdot 3333\ldots$$

The reader is asked to prove that R/Z, + is a group. (This group is called *the group of reals modulo* 1.)

Show in particular that

$$-\cdot 22222\ldots = \cdot 77777\ldots$$

Give the general rule for finding the symmetric of a real modulo 1. The neuter of this group is given by

$$0 = \cdot 00000\ldots = \cdot 99999\ldots$$

(e) Let $n \in \omega_0$. Denote the set of fractions of denominator n by $(1/n)Z$. Thus

$$(1/n)Z = \{z/n \mid z \in Z\}$$

Let us consider the elements of $(1/n)Z$ modulo 1; i.e. each of the fractions z/n will be thought of "with its integral part removed". When this is the case, we shall denote (here only) this fraction by $\frac{z}{n}$. We therefore have in particular

$$\frac{3}{2} = \frac{1}{2} = \cdot 5000\ldots$$

$$\frac{8}{3} = \frac{2}{3} = \cdot 6666\ldots$$

We put

$$0 = \cdot 000\ldots = \frac{0}{n}$$

We shall denote by Z_n the set of elements of $(1/n)Z$ considered modulo 1. Thus

$$Z_2 = \left\{0, \frac{1}{2}\right\}$$

$$Z_3 = \left\{0, \frac{1}{3}, \frac{2}{3}\right\}$$

$$Z_4 = \left\{0, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}\right\}$$

$$Z_n = \left\{0, \frac{1}{n}, \frac{2}{n}, \ldots \frac{n-1}{n}\right\}$$

The reader is asked to establish the rules of combination of Z_n, + and to show that every Z_n, + is a group.

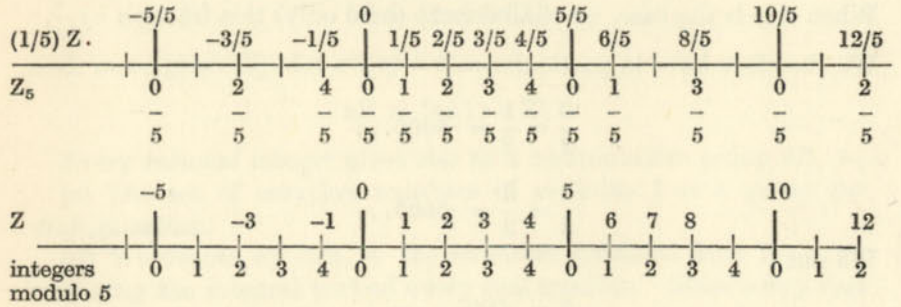
The element $\frac{a}{n}$ may always be written $\frac{r}{n}$ where the numerator r is the remainder after dividing a by n. In the group Z_n, with the number n fixed, every element $\frac{a}{n}$ is determined by the numerator a, or, better still, by the remainder of the division of a by n. We express this result by saying that:

To consider the fractions z/n modulo 1 is equivalent to considering the integers modulo n.

In symbols:

$$\frac{a}{n} = \frac{b}{n} \Leftrightarrow n \mid (a - b)\dagger$$

What does the following diagram suggest to you?



† Tr. See Ch. 6, §5.

(f) Let E be a non-empty set. We know that $\cap$ and $\cup$ are associative, commutative inner laws of $\mathscr{P}E$, but that neither $\mathscr{P}E$, $\cap$ nor $\mathscr{P}E$, $\cup$ are groups. Then again, $\setminus$ is an inner law of $\mathscr{P}E$, everywhere defined but not associative. Thus $\mathscr{P}E$, $\setminus$ is not a group.

We shall show that we can nevertheless combine the operations of union and difference in such a way as to obtain a group law Δ for $\mathscr{P}E$.

Let us define

$$\forall A, B \in \mathscr{P}E: \qquad A \triangle B = (A \setminus B) \cup (B \setminus A) \qquad (1)$$

Thus $A \triangle B$ is the set of elements which belong to one and only one of the sets A and B.

We also have

$$A \triangle B = (A \cup B) \setminus (A \cap B)$$

The reader should establish that $\mathscr{P}E$, $\triangle$ is a group. Bearing in mind formula (1), we often call the law $\triangle$ *the symmetric difference.*

Show that $A_1 \triangle A_2 \triangle \ldots \triangle A_n$ is the set of x such that we have "$x \in A_i$" for an odd number of values of the index i.

We could then write, to amuse ourselves,

$$A_1 \triangle A_2 \triangle \ldots \triangle A_n = \{x \mid 2 + \#\{i \mid x \in A_i\}\}\dagger$$

Point out the neutral element of the group $\mathscr{P}E$, $\triangle$ and the symmetric of $A \subset E$ (in the group $\mathscr{P}E$, $\triangle$).

(g) The symmetric group of a set. We define the symmetric group of a set E to be the set of permutations of E provided with the product of composition. We recall that a permutation of E is *any relation f of* E *to* E *such that every element of* E *is the origin of one and only one pair of f, and the end-point of one and only one pair of f.*†

The identical transformation is thus a permutation of E, and is the neutral element for the product of composition.

If f is a permutation of E, then so is the inverse relation f^{-1}. Since $f \circ f^{-1} = f^{-1} \circ f =$ the identical transformation of E, we have shown that each of the permutations f and f^{-1} is the symmetric of the other for the product of composition $\circ$. The reader should establish that the product of composition (or composite) of two permutations is a permutation and that this law $\circ$ is associative.

We shall have proved in this way that the set of permutations of

† Tr. See Appendix.

E is a group for the product of composition. This group is called the symmetric group of E.

We shall denote the set of permutations of E by E! or $\mathscr{S}$E. Thus the symmetric group of E will be denoted by E!, $\circ$ or $\mathscr{S}$E, $\circ$ (and, by abbreviation, simply $\mathscr{S}$E or E!).

(h) Determine the groups amongst the following structures and justify your answer.

$\{1, -1\}, .$
$\mathrm{R}^-, .$
$\{1, -1, i, -i\}, .$

§6. GENERAL ASSOCIATIVITY

Let G, $*$ be a group. Let $x_1, x_2, \ldots, x_n$ be elements of G. Consider the expression (or term)

$$x_1 * x_2 * \ldots * x_n \tag{1}$$

A priori this expression is meaningless. We may try to give it a meaning by reducing it to a sequence of operations acting on two elements of G. But this may, in general, be done in several ways. Thus, if $n = 4$, we may consider the following sequences of operations on two elements, shown clearly by the brackets.

$$((x_1 * x_2) * x_3) * x_4$$
$$(x_1 * x_2) * (x_3 * x_4)$$
$$(x_1 * (x_2 * x_3)) * x_4$$
$$x_1 * (x_2 * (x_3 * x_4))$$
$$x_1 * ((x_2 * x_3) * x_4)$$

If $n = 3$, there are two possibilities, $(x_1 * x_2) * x_3$ and $x_1 * (x_2 * x_3)$, but we know by the hypothesis of associativity that these two sequences of binary operations give the same final result.

For $n = 2$, there is only one possibility.

For $n = 1$, we shall use the convention that an operation reduced to a single term x has this term as its result.

Thus we see that for $n = 1, 2, 3$ the operation (1) leads to the same result whichever way we insert the brackets. We shall prove, by induction, that this is also true for every n. It will then be quite natural to denote this result by expression (1) (which will therefore have a meaning independent of the way in which we insert the brackets).

The induction which we shall use is of a slightly unusual kind.

The number n having been fixed, we assume that the property is established for all expressions (1) consisting of at most $(n - 1)$ terms (induction hypothesis).

Let us consider a way of inserting the brackets, and let us confine ourselves to inserting the last brackets to be introduced into expression (1).

For example, let

$$s = (x_1 * \ldots * x_m) * (x_{m+1} * \ldots * x_n) \tag{2}$$

It is perfectly legitimate to omit the inner brackets. In fact, there appear inside the brackets of (2) expressions analogous to (1) but consisting of $m < n$ and $n - m < n$ terms respectively. Therefore, by the induction hypothesis, these expressions have a meaning independent of the way the brackets are inserted.

If $m = 1$, expression (2) is of the form

$$x_1 * (x_2 * \ldots * x_n)$$

If $m > 1$, we introduce brackets in the first term of (2)

$$s = (x_1 * (x_2 * \ldots * x_m)) * (x_{m+1} * \ldots * x_n)$$

Again, $(x_2 * \ldots * x_m)$ is meaningful since this expression consists of $m - 1 < n$ terms.

We now apply the associativity property to the product of the three terms x_1, $(x_2 * \ldots * x_m)$, $(x_{m+1} * \ldots * x_n)$.

We get

$$s = x_1 * ((x_2 * \ldots * x_m) * (x_{m+1} * \ldots * x_n))$$

The product $(x_2 * \ldots * x_m) * (x_{m+1} * \ldots * x_n)$ consists of a total of $n - 1 < n$ terms; therefore, by the induction hypothesis, it is quite unnecessary to put in the brackets.

Thus we have established that, if s is the product obtained by inserting the brackets in one way, we always have

$$s = x_1 * (x_2 * \ldots * x_n)$$

Hence all ways of inserting brackets lead to the same result.

Q.E.D.

Exercise

In a group G, $*$ we have

$$\overline{(x * y * \ldots * z)} = \bar{z} * \ldots * \bar{y} * \bar{x}$$

for every $x, y, \ldots, z \in$ G, the bar denoting the symmetric.

Revision exercises on Chapters 1 and 2

1. We give below a list of sets provided with a law. Decide in each case whether the law is everywhere defined, whether it is associative, whether it admits a neutral element, and which are the symmetrizable elements (those which possess a symmetric); also determine in each case whether the law is commutative.

ω, +
ω, −
ω, .
ω, : †
ω_0, +
ω_0, −
ω_0, .
ω_0, :
$2\omega_0$, +
$2\omega_0$, −
$2\omega_0$, .
$2\omega_0$, :
Z, +
Z, −
Z, .
Z, :
Q, +
Q, .
Q_0, .
R, +
R, .
R_0, .
C, +
C, .
C_0, .
ω, $\vee$ (see ch. 2 §4 (j))
ω, $\wedge$
ω_0, $\vee$
ω_0, $\wedge$
$\mathscr{P}E$, $\cap$
$\mathscr{P}E$, $\cup$
$\mathscr{P}E$, $\setminus$
$\mathscr{P}E$, $\triangle$ (where $\triangle$ denotes the symmetric difference).

2. As usual, we denote the set of subsets of the set E by $\mathscr{P}E$.

(a) Prove that the law $\cup$ is associative, commutative and idempotent;‡ does it admit a neutral element?
(b) Use proposition 4 of chapter 1 to show that $\mathscr{P}E$, $\cup$ is a group if and only if $E = \varnothing$.

(c) Prove that E is an absorbant for the law $\cup$, i.e.

$$\forall A \in \mathscr{P}E: \quad A \cup E = E \cup A = E$$

(d) Prove that $\cup$ is autodistributive, i.e.

$$\forall A, B, C \in \mathscr{P}E: \quad A \cup (B \cup C) = (A \cup B) \cup (A \cup C)$$

† Tr. $a : b$ = ratio of a to b = a/b in the usual notation.
‡ Tr. i.e. every element is an idempotent for this law.

(e) $\cup$ is commutassociative:

$$\forall A, B, C, D \in \mathscr{P}E: \quad (A \cup B) \cup (C \cup D) = (A \cup C) \cup (B \cup D)$$

(f) $\forall A, B, C \in \mathscr{P}E: \quad (A = B) \Rightarrow (A \cup C = B \cup C)$
(g) $\cup$ does not allow cancellation.
(h) $\forall A, B, C \in \mathscr{P}E: \quad (A \subset B) \Rightarrow (A \cup C \subset B \cup C)$.
(i) $\forall A, B, C, D \in \mathscr{P}E: \quad ((A \subset B) \text{ and } (C \subset D)) \Rightarrow (A \cup C) \subset (B \cup D)$.

3. Study $\mathscr{P}E$, $\cap$ in a way analogous to that of exercise 2.

4. $\forall A, B \in \mathscr{P}E$:

$$A \cap (A \cup B) = A,$$
$$A \cup (A \cap B) = A$$

5. Let Π be a plane. Let us define the law $*$ as follows:

$$\forall a, b \in \Pi: \quad a * b = \text{the middle of the segment } [a, b].$$

Is the law $*$ associative, commutative, idempotent? Does it admit a neutral element? Does the structure Π, $*$ constitute a group?

6. The law − is not associative in R, nor in Z, nor in ω, nor in ω_0.

7. Are the following laws associative?

(a) $\omega_0 \times \omega_0 \to \omega_0$: $(x, y) \to x^y$,†
(b) $Z \times Z \to Z$: $(x, y) \to \max(x, y)$,
(c) $R^+ \times R^+ \to R^+$: $(x, y) \to x^y$.

8. Let E be provided with a law $\triangle$ everywhere defined and associative. Let a be a fixed element of E. Prove that the law $*$ defined by

$$\forall x, y \in E: \quad x * y = x \triangle a \triangle y$$

is associative.

9. The set E is provided with the laws $*$ and $\perp$ defined as follows:

(a) $\forall x, y \in E: \quad x * y = x$;
(b) $\forall x, y \in E: \quad x \perp y = y$.

Prove that both these laws are associative.

† Tr. See Appendix.

10. Are the following laws associative? commutative? Do they allow cancellation? Do they admit a neutral element?

(a) $\omega \times \omega \to \omega$: $(x, y) \to x + y$
(b) $\omega \times \omega \to \omega$: $(x, y) \to x^2 + y^2$
(c) $\omega \times \omega \to \omega$: $(x, y) \to x^3 + y^3$
(d) $\omega \times \omega \to \omega$: $(x, y) \to x(x + y)$.

11. Let E be a set provided with the law $*$. Denote by P the subset

$$\{x \in \mathrm{E} \mid \forall y, z \in \mathrm{E}: \quad x * (y * z) = (x * y) * z\}$$

Prove that: $a, b \in \mathrm{P} \Rightarrow a * b \in \mathrm{P}$. The law $*$ is associative in P.

12. Another example of a law which is not everywhere defined: We denote by $\mathscr{S}$ the set of segments $[a, b]$ of the real straight line $(a \leqslant b)$. Our law, which we shall write additively, is defined for the pairs $([a, b], [c, d])$, when $b = c$. We then put:

$$[a, b] + [b, d] = [a, d]$$

Thus $\mathscr{S}$, $+$ is a set with a law not everywhere defined.

Since this law is not everywhere defined, it is not associative (see the definition of associativity). Nevertheless, let $[a, b]$, $[c, d]$, $[e, f] \in \mathscr{S}$; assume that

$$([a, b] + [c, d]) + [e, f]$$

is defined. What can you say about

$$[a, b] + ([c, d] + [e, f])?$$

13. Denote by E^{E} the set of transformations of E (i.e. the set of maps $\mathrm{E} \to \mathrm{E}$). Is the law $\circ$ (product of composition) associative? Does it admit a neuter?

14. Let us consider the two laws:

(a) $\omega \times \omega \to \omega$: $(x, y) \to \max(x, y)$,
(b) $\mathrm{Z} \times \mathrm{Z} \to \mathrm{Z}$: $(x, y) \to \max(x, y)$.

Are these laws associative? Do they admit a neuter?

15. The laws

(a) $\mathrm{Z} \times \mathrm{Z} \to \mathrm{Z}$: $(x, y) \to x - y$
(b) $\omega \times \omega \to \omega$: $(x, y) \to x^y = x * y$

have a right neuter, but not a left neuter. Find this right neuter in both cases.

16. An example of a law which admits several right neuters. Let us provide Z with the law $*$ defined as follows:

$$\begin{cases} x * y = x + y, & \text{when } y \geqslant 0; \\ x * y = x, & \text{when } y < 0. \end{cases}$$

What are the right neuters? Does this law admit a left neuter?

17. In ω, $+$ and ω, . the neuter is the only symmetrizable element.

18. Which is the only symmetrizable element in

(a) Q, .
(b) R, .
(c) C, .
(d) $\mathrm{Z} \setminus \{1\}$, $+$
(e) $\mathrm{Z} \setminus \{-1\}$, $+$

19. Consider the structure E, $*$ where $*$ is an associative law admitting a neutral element. Show that this neuter is necessarily unique. How would you define the symmetrizable elements of E, $*$? Show that every symmetrizable element x admits a unique symmetric which we shall denote by $\bar{x}$. Show that if x and y are symmetrizable, then so is $x * y$, and that $\overline{x * y} = \bar{y} * \bar{x}$.

20. In the set E^{E} of transformations of the set E, the symmetrizable elements for the law $\circ$ (the product of composition) are the permutations. If t is a symmetrizable transformation of E, the reciprocal transformation of t is the symmetric of t.

21. In M, $*$, every element $a \in \mathrm{M}$ such that

$$\forall m \in \mathrm{M}: \quad a * m = a = m * a$$

is called an absorbent. Prove that every absorbent is idempotent; but that the reciprocal is false.

22. Prove that the following structures are groups.

(a) Z, $+$
(b) Q, $+$
(c) R, $+$
(d) C, $+$
(e) Q_0^+, .
(f) R_0^+, .

(g) $C_0, .$
(h) $\mathscr{P}E, \Delta$
(i) $\{1, i, -1, -i\}, .$
(j) $\{2^m \mid m \in Z\}, .$
(k) $\left\{\frac{1+2m}{1+2n} \mid m, n \in Z\right\}, .$

23. Which of the following structures are groups?

(a) $\mathscr{P}E, \cup$
(b) $\mathscr{P}E, \cap$
(c) $\{\cos\theta + i \sin\theta \mid \theta \in Q\}, .$
(d) $2Z, +$
(e) $2Z, .$
(f) $2Z + 1, +$
(g) $2Z + 1, .$
(h) The set of irrational numbers for multiplication
(i) $\{z \in C \mid |z| = 1\}, .$
(j) $\{z \in C \mid |z| = 1\}, *$, where $*$ is defined as follows: $z_1 * z_2 = |z_1| \cdot z_2$.

24. The set of plane rotations about a fixed point forms a group for the product of composition.

25. Denote by A the set of n n^{th} roots of 1. Prove that A, . is a group.

26. Denote by $\mathscr{T}$ the set of translations of the plane. Prove that $\mathscr{T}, \circ$ is a group.

27. Let G, $*$ be a group; let $a, b \in G$. If $a * a = b * b = (a * b) * (a * b) = \nu$, then $a * b = b * a$ (ν denotes the neuter of G, $*$).

28. Direct sum

Let G, + and H, + be two additive groups. We provide the product-set $G \times H = \{(a, b) \mid a \in G, b \in H\}$ with the law + defined thus:

$$\forall (a, b), (c, d) \in G \times H: \qquad (a, b) + (c, d) = (a + c, b + d)$$

Prove that $G \times H, +$ is a group (the direct sum of G and H). What is its neuter? What is the symmetric of (a, b)? We denote the direct sum of G and H by $G \oplus H$.

29. Direct product

If G, . and H, . are two multiplicative groups, construct the direct product of G and H by analogy with Ex. 28.

We denote the direct product of G and H by $G \otimes H$.

30. Provide $R_0 \times R$ with a law . by defining

$$\forall (a, b), (c, d) \in R_0 \times R: \qquad (a, b) \cdot (c, d) = (ac, bc + d)$$

Prove that $R_0 \times R, .$ is a group. What is its neuter? What is the inverse of (a, b)?

31. Decide whether the elements of Z form a group for the following laws.

(a) $a * b = a + b$
(b) $a * b = 2(a + b)$
(c) $a * b = a - b$
(d) $a * b = 2a + b$
(e) $a * b = 2a + b - a^2$.

32. The same question for 2Z.

33. Let G, $*$ be a group. Prove that the map

$$b : G \to G : g \to \bar{g}$$

is a bifunction.†

34. In every group G, $*$ we have

$$\forall a, b, c \in G, \exists x \in G: \qquad a * b * x * a * x = c * b * x$$

35. Let $a, b, c, d \in C$. Prove that the set of transformations

$$C \to C: \qquad x \to \frac{ax + b}{cx + d}, \text{ with } ad - bc = 1$$

is a group for the product of composition.

36. What are the commutative symmetric groups?

37. For every group G, $*$, the centre of G, which we denote by Z_G, is defined as the set of elements of G which commute with all the elements of G:

$$Z_G = \{z \in G \mid \forall x \in G: \quad z * x = x * z\}$$

Prove that the centre of every group is a subgroup of this group.

38. $\{1, 2, 3\}!, \circ$ is a group whose centre reduces to the sole unit-element.

39. The same is true for the group $\{1, 2, 3, 4\}!, \circ$.

40. A group is equal to its centre if and only if it is commutative.

† Tr. See Appendix.

41. Multiplication table

Let G, $*$ be a finite group with n elements. This group is known as long as we know the n^2 products $a * b$ of the elements of G. CAYLEY saw the advantage of having a multiplication table to determine a finite group (1854). We give below some examples of groups defined by a CAYLEY multiplication table; it is instructive to verify in each case that we are indeed dealing with a group.

(a) The cyclic group Z_5, $+$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

For example: to find $3 + 2$ we look for the element at the intersection of the 4th line and 3rd column, and we conclude that: $3 + 2 = 0$. At the same time we see that: $-3 = 2$, $-2 = 3$.

(b) The cyclic group Z_2, $+$

$+$	0	1
0	0	1
1	1	0

(c) $\{1, -1, i, -i\}$, $\cdot$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(d) The quaternion group: $\mathcal{Q}$, .

$\cdot$	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

(e) KLEIN'S four-group: V, $*$

$*$	1	a	b	$a*b$
1	1	a	b	$a*b$
a	a	1	$a*b$	b
b	b	$a*b$	1	a
$a*b$	$a*b$	b	a	1

42. Every group of 4 or fewer than 4 elements is commutative. (Clue: it is profitable to use a CAYLEY table.)

43. Let a, b be elements of a group G, $*$.

If: $\bar{a} * b * a = \bar{b}$

and $\bar{b} * a * b = \bar{a}$,

then: $a * a * a * a = b * b * b * b = \nu$.

44. No subset of Z of more than 2 elements is a multiplicative group.

45. Construct the multiplication table of the multiplicative group whose elements are

$$1, a, a^2, a^3, b, c, d, e,$$

where:

$$c = ab, \quad d = a^2b, \quad e = a^3b, \quad a^4 = 1, \quad b^2 = 1, \quad ba = a^3b.$$

Determine the subgroups of this group.

3

The Scalar Law of a Group

§1. INTRODUCTION

The law $*$ of the group G, $*$ is an inner law of G, i.e. a map

$$G \times G \to G : (x, y) \to x * y$$

We shall see that, given only the group G, $*$, we can define a law

$$Z \times G \to G$$

which we shall call the scalar law of G.

In this law, the first term is a rational integer. The second term and the result are elements of the group.

We say that the scalar law is an outer law of G, and that Z is its set of operators.

In the case of the group G, $*$ we shall denote the scalar law by means of the symbol $\perp$.

We shall see later the usual notations for additive and multiplicative groups.

For a group G, $*$ we then have

$$\perp : Z \times G \to G : (z, g) \to z \perp g$$

It is time to define the law $\perp$.

§2. THE OUTER LAW: $\omega_0 \times G \to G$

For every $n \in \omega_0$ and for every $g \in G$, we shall put

$$n \perp g = \underbrace{g * g * \ldots * g}_{n \text{ terms}} \tag{1}$$

In particular:

$$1 \perp g = g \tag{2}$$

As an exercise, the reader is asked to establish the truth of the formula

$$\forall m, n \in \omega_0;\ \forall g \in G: \qquad (m + n) \perp g = (m \perp g) * (n \perp g) \tag{3}$$

§3. THE SCALAR LAW OF THE GROUP G, $*$

We shall extend the law defined above to a law $Z \times G \to G$ which will be called the scalar law of the group G, $*$.

Let us start by defining

$$\forall g \in G: \qquad 0 \perp g = \nu \tag{1}$$

Before defining $(-n) \perp g$, (with $n \in \omega_0$ and $g \in G$) let us show that

$$\overline{(n \perp g)} = n \perp \bar{g} \tag{2}$$

We have

$$\begin{aligned} \overline{(n \perp g)} &= \overline{(g * g * \ldots * g)} && \text{(definition §2.1)} \\ &= \bar{g} * \bar{g} * \ldots * \bar{g} && \text{(property Ch. 2 §6)} \\ &= n \perp \bar{g} && \text{(definition §2.1)} \end{aligned}$$

It is then natural to put

$$(-n) \perp g = n \perp \bar{g} = \overline{n \perp g} \tag{3}$$

which completes the definition of the scalar law.

In particular

$$\begin{aligned} (-1) \perp g &= 1 \perp \bar{g} && \text{(by (3))} \\ &= \bar{g} && \text{(by §2.2)} \end{aligned}$$

Therefore

$$(-1) \perp g = \bar{g} \tag{4}$$

Hence (3) gives

$$(-n) \perp g = n \perp ((-1) \perp g) = (-1) \perp (n \perp g) \tag{5}$$

§4. PROPERTIES OF THE SCALAR LAW

We shall leave to the reader the task of proving the law of composition.

> In every group G, $*$:
> $\forall a, b \in Z;\ \forall g \in G: \qquad (a + b) \perp g = (a \perp g) * (b \perp g) \qquad (1)$

§5. SUPPLEMENTARY PROPERTIES OF THE SCALAR LAW IN THE CASE OF A COMMUTATIVE GROUP G, $*$

If the group G, $*$ is commutative, we have

$$\forall n \in \omega_0;\ \forall x, y \in G: \qquad n \perp (x * y) = (n \perp x) * (n \perp y) \tag{1}$$

In fact

$$\begin{aligned} n \perp (x * y) &= (x * y) * \ldots * (x * y) && \text{(definition §2.1)} \\ &= (x * \ldots * x) * (y * \ldots * y) && \text{(associativity and commutativity of } *) \\ &= (n \perp x) * (n \perp y) && \text{(definition §2.1)} \end{aligned}$$

By definition (§3.1) we also get

$$0 \perp (x * y) = (0 \perp x) * (0 \perp y) \qquad (2)$$

Exercise

Prove formula (2).

Finally, we prove that we also have

$$\forall n \in \omega_0;\ \forall x, y \in \mathrm{G}: \quad (-n) \perp (x * y) = ((-n) \perp x) * ((-n) \perp y) \qquad (3)$$

In fact

$$\begin{aligned} (-n) \perp (x * y) &= n \perp \overline{(x * y)} && \text{(definition §3.3)} \\ &= n \perp (\bar{x} * \bar{y}) && \text{(by (Ch. 2, §6.1) and the commutativity of } *) \\ &= (n \perp \bar{x}) * (n \perp \bar{y}) && \text{(by (1))} \\ &= ((-n) \perp x) * ((-n) \perp y) && \text{(definition §3.3)} \end{aligned}$$

Q.E.D.

Bringing together formulae (1), (2) and (3), we get

In every commutative group G, $*$:

$$\forall a \in \mathrm{Z};\ \forall x, y \in \mathrm{G}: \quad a \perp (x * y) = (a \perp x) * (a \perp y) \qquad (4)$$

§6. THE SCALAR LAW IN A GROUP G, .

In the case of a group given by G, ., we write x^a instead of $a \perp x$ (for all $a \in \mathrm{Z}$ and $x \in \mathrm{G}$). We then have, for every $n \in \omega_0$,

$$x^n = \underbrace{x \,.\, x \,.\, \ldots x}_{n \text{ factors}}, \quad x^0 = 1, \quad x^{-n} = (x^n)^{-1} = (x^{-1})^n \qquad (1)$$

The elements x^a (with $a \in \mathrm{Z}$) are called powers of the element $x \in \mathrm{G}$.

Rule (§4.1) becomes here the famous rule of exponents.

In every group G, .

$$\forall a, b \in \mathrm{Z};\ \forall x \in \mathrm{G}: \quad x^{a+b} = x^a \,.\, x^b \qquad (2)$$

If the group is commutative, we have, in addition, the rule

In every commutative group G, .

$$\forall a \in \mathrm{Z};\ \forall x, y \in \mathrm{G}: \quad (x \,.\, y)^a = x^a \,.\, y^a \qquad (3)$$

§7. THE SCALAR LAW OF A GROUP G, +

In the case of a group G, +, the result of the scalar law is denoted by ax instead of $a \perp x$.

We therefore have (for every $n \in \omega_0$),

$$nx = \underbrace{x + \ldots + x}_{n \text{ terms}}; \quad 0x = 0; \quad (-n)x = -(nx) = n(-x) \qquad (1)$$

In the formula $0x = 0$, the first symbol 0 denotes the natural number zero (belonging to Z), while the second symbol 0 denotes the neuter of the group G, +.

The elements ax are called (whole) multiples of x.

Rule (§4.1) becomes here

In every group G, +

$$\forall a, b \in \mathrm{Z};\ \forall x \in \mathrm{G}: \quad (a + b)x = ax + bx \qquad (2)$$

If the group G, + is commutative, we have in addition,

In every commutative group G, +

$$\forall a \in \mathrm{Z};\ \forall x, y \in \mathrm{G}: \quad a(x + y) = (ax) + (ay) \qquad (3)$$

§8. THE SCALAR LAW IN THE SYMMETRIC GROUP $\mathscr{S}\mathrm{E}, \circ$ OF THE SET E

For the law $\circ$ we adopt the usual conventions of multiplicative groups (i.e. groups whose law is written .). According to the circumstances, we represent the identical permutation of E by 1, or by I, or by ϵ. It is the neutral element of the group.

We recall that f^{-1} denotes the reciprocal permutation of the

permutation $f \in \mathscr{S}\mathrm{E}$. The elements f and f^{-1} of the group $\mathscr{S}\mathrm{E}, \circ$ are symmetrics or inverses. Following the usual conventions, we put

$$f^{-n} = (f^n)^{-1} = (f^{-1})^n; \qquad f^0 = 1$$

§9. MIXED ASSOCIATIVITY

We shall give a definition later of multiplication of rational integers, thus promoting Z into a structure with two laws

$$\mathrm{Z}, +, .$$

But now we describe the rule of mixed associativity which applies simultaneously to scalar multiplication and to multiplication in Z:

$$\forall a, b \in \mathrm{Z}, \forall g \in \mathrm{G}: \qquad a \perp (b \perp g) = (a \,.\, b) \perp g \qquad (1)$$

This law will be proved later as an exercise.

§10. EXERCISES

1. In a group G, ., mixed associativity is expressed as

$$\forall a, b \in \mathrm{Z}, \forall g \in \mathrm{G}: \qquad (g^b)^a = g^{ab}$$

Since multiplication in Z is in fact commutative, we can again write

$$\forall a, b \in \mathrm{Z}, \forall g \in \mathrm{G}: \qquad (g^a)^b = g^{ab}$$

2. In the case of a group M, +, mixed associativity is written

$$\forall a, b \in \mathrm{Z}, \forall m \in \mathrm{M}: \qquad a(bm) = (a \,.\, b)m$$

3. In the group R/Z, +, put

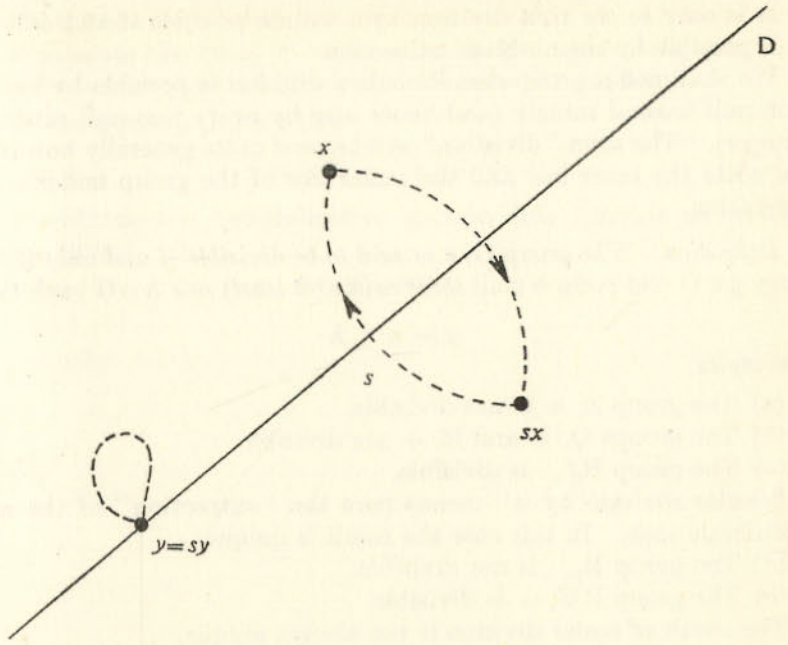
$$\cdot 1111 \ldots = r$$

Then we get

$$\begin{aligned} 9r &= 0 \\ 10r &= r \\ 8r &= -r \end{aligned}$$

4. If s denotes the symmetry of the plane Π with respect to the straight line D contained in Π, we have the formulae

$$\begin{aligned} s \circ s &= 1 \\ s &= s^{-1} \\ s^2 &= 1 \\ s^{17} &= s \\ s^{-18} &= 1 \end{aligned}$$



5. The scalar law of the group Z, + is none other than ordinary multiplication in Z.

§11. DIVISIBLE GROUPS

Let M, + be an additive group.

Its scalar law allows us to "multiply" scalarly every element $m \in \mathrm{M}$ by every rational integer $z \in \mathrm{Z}$. The result of this operation is the integral multiple zm of m.

Quite naturally, the question arises of "scalar division" by z. In other words, given $w \in \mathrm{M}$, does there always exist an element $v \in \mathrm{M}$ such that $zv = w$?

The example of the group Z, + of rational integers is sufficient to prove that "scalar division" by z is not always possible.

The example of the group R/Z, + shows that, when this operation is possible, it is not always unique.

Example: $3 \,.\, (\cdot 000 \ldots) = 0$
$3 \,.\, (\cdot 333 \ldots) = 0$
$3 \,.\, (\cdot 666 \ldots) = 0$

It is easy to see that division by z will be possible if and only if it is possible by the absolute value of z.

We shall call a group *divisible* when division is possible by every non-null natural integer (and hence also by every non-null rational integer). The term "divisible" will be used quite generally however we write the inner law and the scalar law of the group under consideration.

Definition. The group $G, *$ *is said to be divisible if and only if for every* $g \in G$ *and every* $n \in \omega_0$ *there exists (at least) one* $h \in G$ *such that*

$$g = n \perp h$$

Examples

(a) The group Z, + is not divisible.

(b) The groups Q, + and R, + are divisible.

(c) The group $R_0^+, .$ is divisible.

"Scalar division by n" means here the "extraction" of the n^{th} arithmetic root. In this case the result is unique.

(d) The group $R_0, .$ is not divisible.

(e) The group R/Z, + is divisible.

The result of scalar division is not always unique.

(f) The group of plane rotations about a point is divisible. The result of scalar division is not always unique.

Exercises

1. Investigate the groups you know to decide which are divisible and which are not.

2. When a group $G, *$ is divisible with unique scalar division, it is natural to denote by

$$(1/n) \perp g$$

the result of "the scalar division" of g by n. In the case of a multiplicative group $G, .$, this result is written $g^{1/n}$.

We thus arrive quite naturally at rational exponents.

The reader should show with details that, in a divisible group $G, *$ with unique scalar division, we can define naturally an outer law

$$Q \times G \to G: \qquad (a/b, g) \to (a/b) \perp g$$

Establish the properties of such a law:

(1) in the case of any group whatsoever,

(2) in the case of a commutative group.

Formulate the rules of combination in the case of a group $G, *$, also for a multiplicative group and for an additive group.

(3) In a group $G, *$ we have

$$\forall z \in Z: \qquad z \perp \nu = \nu$$

For additive and multiplicative groups, this formula is written respectively

$$z \,.\, 0 = 0 \quad \text{and} \quad 1^z = 1$$

4

Subgroups

§1. EXAMPLE

The set Q (see Ch. 2 §3) is a subset of the group R, +. The sum of two elements of Q belongs to Q, and Q, + is itself a group (for the law + defined in Q as well as in R).

We shall say that Q, + is a subgroup of the group R, +.

Similarly, Z, + is a subgroup of Q, +, and R_0, . is a subgroup of C_0, .. Finally, Z_n, + is a subgroup of R/Z, +.

§2. STABLE SUBSETS AND SUBGROUPS

Let G, $*$ be a group and P a subset of G. The subset P of G is said to be stable for $*$ if and only if

$$x, y \in P \Rightarrow x * y \in P \qquad (1)$$

Examples

Q is a stable subset of R, +
Z is a stable subset of Q, +
R_0 is a stable subset of C_0, .
ω is a stable subset of Z, +

If P is a stable subset of G, $*$, we can speak without ambiguity of P, $*$, since the law $*$ is everywhere defined in P by (1).

The associativity of the law $*$ in G guarantees its associativity in P.

Exercise

Justify the above claim.

Similarly, if $*$ is commutative in G its commutativity implies that of $*$ in P.

Meanwhile we note that P can be a stable subset of G, $*$ without P, $*$ being a group (as is shown in particular in the case of the stable subset ω of Z, +).

Definition. Every stable subset S *of a group* G, $*$ *such that* S, $*$ *is a group is called a subgroup of* G, $*$.

We shall sometimes indicate that P, $*$ is a subgroup of G, $*$ by writing

$$P, * \subset G, *$$

Often we simply write

$$P \subset G$$

Exercises

1. Here are some subsets of Z which are stable for addition:

$$\begin{aligned}
\omega &= \{0, 1, 2, \ldots\} \\
-\omega &= \{0, -1, -2, \ldots\} \\
\omega_0 &= \{1, 2, 3, \ldots\} \\
-\omega_0 &= \{-1, -2, -3, \ldots\} \\
2\omega &= \{0, 2, 4, 6, \ldots\} \\
a\omega &= \{0, a, 2a, 3a, \ldots\} \\
\omega \setminus \{0, 1, 2\} &= \{3, 4, 5, \ldots\} \\
-(\omega_0 \setminus \{1\}) &= \{-2, -3, -4, -5, \ldots\} \\
8\omega_0 &= \{8, 16, 24, \ldots\} \\
&Z \\
&\{0\}
\end{aligned}$$

Is this still true of the following subsets?

$$\begin{aligned}
\{-1, 0, 1, 2, \ldots\} &= \omega \cup \{-1\} \\
(-\omega) \cup \{1\} &= \{1, 0, -1, -2, \ldots\} \\
&\{-3, -2, -1, 0, 1, 2, 3, \ldots\} \\
&\{2\} \\
&\{-3, 5\}
\end{aligned}$$

2. The set L of terminating decimals

$$L = \{a/10^n \mid a \in Z, n \in \omega\}$$

is a subgroup of Q, +.

The set $L \setminus \{0\}$ is a stable subset of Q_0, ., but it is not a subgroup of Q_0, ..

3. In Z_6, +, the set $\left\{\overline{0}, \overline{2}, \overline{4}\right\}$ is stable for addition and subtraction, and it is a subgroup of Z_6, +.

4. In the symmetric group $\mathcal{S}\Pi$, $\circ$ of the plane Π, every pair $\{1, s\}$ where 1 denotes the identical transformation and s a symmetry of

the plane (either with respect to a straight line or with respect to a point) is a subgroup of $\mathscr{P}\Pi, \circ$.

§3. THE NEUTRAL ELEMENT AND THE SYMMETRIC IN A SUBGROUP

Let P, $*$ be a subgroup of G, $*$.

Denote by ν' the neutral element of P, $*$. We then have

$$\nu' * \nu' = \nu' \tag{1}$$

which establishes the idempotence of ν'. Now, we know (chapter 1, proposition 4) that the neutral element of G, $*$ is the only idempotent of G, $*$. Hence, $\nu' = \nu$. Thus, the neutral element of a group is the neutral element of each of its subgroups.

We shall show that the same is true of the symmetric. Let x be an element of P. Let us denote its symmetric in P, $*$ by x'. Then

$$x' * x = \nu = x * x' \tag{2}$$

Since the symmetric in G, $*$ is unique, we conclude that $x' = \bar{x}$, which allows us to enunciate.

Theorem 1 – *The neutral element of a subgroup coincides with that of the group, and the symmetric in the subgroup of an element of the subgroup coincides with its symmetric in the group.*

§4. A NEW CHARACTERIZATION OF SUBGROUPS

Theorem 2 – *A non-empty subset of a group is a subgroup if and only if it is stable for one of the inverse laws of the group.*

Let G, $*$ be a group and let us consider the inverse law $\bar{*}$ (Ch. 1 §6).

If S is a subgroup of G, then for every $a, b \in S$, the equation

$$x * b = a \tag{3}$$

has a solution in S. Since equation (3) admits the unique solution

$$x = a \bar{*} b \tag{4}$$

in G, $*$, it follows that

$$a, b \in S \Rightarrow a \bar{*} b \in S \tag{5}$$

Conversely, assume that S is a non-empty subset of G such that equation (5) holds for every two elements $a, b \in S$.

Since $S \neq \varnothing$, let

$$s \in S \tag{6}$$

Consequently, by (5)

$$\nu = s \bar{*} s \in S \tag{7}$$

and immediately, by (6), (7) and (5),

$$\bar{s} = \nu \bar{*} s \in S$$

We have just proved that S contains the neuter of G, $*$ and the symmetric (in G, $*$) of every element of S. It remains to prove that S is stable for $*$. Let $u, v \in S$. We then have $\bar{v} \in S$ and consequently (by (5))

$$u * v = u \bar{*} (\bar{v}) \in S$$

Q.E.D.

§5. TRIVIAL SUBGROUPS

Let G, $*$ be a group with neutral element ν. The reader should verify that G and $\{\nu\}$ are subgroups of G, $*$. We call them the trivial subgroups of G, $*$. For every subgroup H of G we have

$$(\{\nu\}, *) \subset (H, *) \subset (G, *)$$

We express this fact by saying that $\{\nu\}$ is the minimum subgroup and G the maximum subgroup of G, $*$.

The maximum subgroup G is also called the improper subgroup of G, $*$.

Exercises in terminology, vocabulary and notation

1. What is the minimum subgroup of R, + ?
2. What is the improper subgroup of C_0, . ?
3. What is the minimum subgroup of R_0, . ?
4. What is the minimum subgroup of the symmetric group of the set $\{1, 2, 3\}$?

Exercises

1. Does the group Z_7, + possess non-trivial subgroups?
2. The same question for Z_6, +.
3. For what values of n does Z_n, + have no non-trivial subgroups? Could you try to justify your answers to the above questions?
4. Investigate the subgroups of the symmetric groups of the sets $\{1, 2\}$, $\{1, 2, 3\}$, $\{1, 2, 3, 4\}$, $\{1, 2, 3, 4, 5\}$.

§6. THE INTERSECTION OF A SET OF SUBGROUPS

Let $\mathscr{F}$ be a non-empty set of subgroups of the group G, $*$. Let us consider the intersection, $\cap\mathscr{F}$, of this set of subsets of G. We therefore denote by $\cap\mathscr{F}$ the set of elements which belong to all the subgroups that are elements of $\mathscr{F}$.

In symbols

$$\cap\mathscr{F} = \{x \in G \mid \forall F \in \mathscr{F}: \quad x \in F\}$$

We shall establish that $\cap\mathscr{F}$ is a subgroup (of G, $*$).
By theorem 2, it is sufficient to show that

$$\forall x, y \in G: \quad x, y \in \cap\mathscr{F} \Rightarrow x \bar{*} y \in \cap\mathscr{F}$$

Now we have successively

$$\begin{aligned} x, y \in \cap\mathscr{F} &\Rightarrow (\forall F \in \mathscr{F}: \ x, y \in F) && \text{(definition of } \cap\mathscr{F}) \\ &\Rightarrow (\forall F \in \mathscr{F}: \ x \bar{*} y \in F) && \text{(since F is stable for } \bar{*}) \\ &\Rightarrow x \bar{*} y \in \cap\mathscr{F} && \text{(definition of } \cap\mathscr{F}) \end{aligned}$$

Q.E.D.

Theorem 3 – *The intersection of every set of subgroups* (*of a group*) *is a subgroup* (*of this group*).

In short: Every intersection of subgroups is a subgroup.

§7. THE SUBGROUP GENERATED BY A SUBSET OF A GROUP

Let G, $*$ be a group and $P \subset G$.† We are going to establish that G contains a subgroup containing P and included in every subgroup of G containing P.

In other words: the set $\mathscr{P}$ of subgroups of G containing P contains a subgroup included in all the subgroups belonging to $\mathscr{P}$. We shall prove that $\cap\mathscr{P}$ is the required subgroup.

Note that $G \in \mathscr{P}$ (since G is a subgroup of G which contains P). Thus $\mathscr{P}$ is a non-empty set of subgroups of G, and consequently, by theorem 3, $\cap\mathscr{P}$ is a subgroup of G.

All the subgroups belonging to $\mathscr{P}$ contain P. The same is therefore true of the intersection of $\mathscr{P}$, and $\cap\mathscr{P}$ is thus a subgroup of G containing P, i.e.

$$\cap\mathscr{P} \in \mathscr{P}$$

† Tr. See §2.

Since $\cap\mathscr{P}$ is, as an intersection, included in all the subgroups belonging to $\mathscr{P}$, it follows that $\cap\mathscr{P}$ is indeed the smallest subgroup of G containing P, which proves our proposition.

The subgroup whose existence we have just established is said to be generated by P. We shall denote it by grp P.

If $P = \{p\}$, we allow ourselves to write grp (p) (even grp p) instead of grp $\{p\}$.

Theorem 4 – *If* P *is a subset of the group* G, $*$, *there exists a subgroup* grp P *of* G, $*$ *containing* P *and included in all the subgroups of* G *containing* P.

The subgroup grp P *of* G, $*$ *is therefore the smallest subgroup of* G, $*$ *which contains* P. *It is necessarily unique and is called the subgroup of* G, $*$ *generated by* P.

Corollaries

1. If A and B are subsets of the group G, $*$,

$$A \subset B \Rightarrow \text{grp } A \subset \text{grp } B$$

2. If S is a subgroup of G, $*$ and P a subset of G, we have grp S = S and

$$P \subset S \Rightarrow \text{grp } P \subset S$$

3. If A and B are subsets of the group G, $*$, then

$$\begin{aligned} \text{grp } (A \cup B) &= \text{grp } ((\text{grp } A) \cup B) \\ &= \text{grp } (A \cup (\text{grp } B)) \\ &= \text{grp } ((\text{grp } A) \cup (\text{grp } B)) \end{aligned}$$

Exercise

In the group G, $*$ we have

$$\text{grp } G = G; \qquad \text{grp } \{e\} = \text{grp } \varnothing = \{e\}$$

§8. MOORE'S CLOSURE

Given a group G, $*$, we have defined a function grp whose domain† is the set $\mathscr{P}G$ of subsets of G and whose image† is the set $\mathscr{G}G$ of subgroups of G, $*$

$$\text{grp } \mathscr{P}G \to \mathscr{G}G: \qquad P \to \text{grp } P$$

(where $\mathscr{P}G$ denotes the set of subsets of G and $\mathscr{G}G$ the set of subgroups of G, $*$).

† Tr. See Appendix.

If A, B denote subsets of G, we have

$$(1)\ A \subset \operatorname{grp} A$$
$$(2)\ A \subset B \Rightarrow \operatorname{grp} A \subset \operatorname{grp} B$$
$$(3)\ \operatorname{grp}\operatorname{grp} A = \operatorname{grp} A$$

We shall express these three properties by saying that the function grp is (1) expanding (2) increasing (3) idempotent. (The term "idempotent" is justified by the formula $\operatorname{grp} \circ \operatorname{grp} = \operatorname{grp}$.)

The function grp is a transformation of $\mathscr{P}G$, i.e. a map $\mathscr{P}G \to \mathscr{P}G$.

A transformation of a set of subsets which is simultaneously expanding, increasing and idempotent is called *a Moore closure*. Thus the transformation of the set of subsets of a group which maps every subset onto the subgroup which it generates is a Moore closure of the set of subsets of the group.

§9. GENERATING SUBSETS

A subset P of the group G, $*$ is said to be *generating* if and only if $\operatorname{grp} P = G$.

Instead of saying that P is a generating subset of G, we sometimes say that P is a set of generators of G. This last expression, although much used, is nevertheless inadvisable because it seems to imply that the generators are special elements of a group. They are nothing of the kind, as the following example shows: {1} and {2, 3} are disjoint generating subsets of Z, +.

Exercises

1. In Z, +, we have

$$\operatorname{grp}(2) = 2\mathrm{Z}$$
$$\operatorname{grp}(n) = n\mathrm{Z}$$
$$\operatorname{grp}(0) = \{0\} = 0\mathrm{Z}$$

2. In the group G, $*$ (whose neutral element is denoted by ν), we have

$$\operatorname{grp} \varnothing = \{\nu\}$$
$$\operatorname{grp}(\nu) = \{\nu\}$$
$$\operatorname{grp} G = G$$

§10. CYCLIC GROUPS

Every group which admits a generating subset consisting of a single element is called a *cyclic group*.

For every subset P of G it is clear that P is a generating subset of the subgroup grp P. Thus the subgroups generated by (a subset reduced to) an element of G are cyclic groups which are therefore the cyclic subgroups of G, $*$. We shall also say that grp (g) is the cyclic subgroup of g.

Since grp (g) is a subgroup, we have $\nu \in \operatorname{grp}\{g\}$

i.e. $$0 \perp g \in \operatorname{grp}\{g\}$$

Since the group grp (g) is stable for the law $*$, we have immediately

$$\forall n \in \omega: \qquad n \perp g \in \operatorname{grp}(g)$$

Since grp (g) is a group, the symmetric $\bar{g}$ of g is an element of grp (g), and consequently the stability of grp g for the law $*$ implies

$$\forall n \in \omega: \qquad (-n) \perp g \in \operatorname{grp}(g)$$

We have thus established that the set $\{z \perp g \mid z \in \mathrm{Z}\}$ is a subset of grp (g) which contains g. Now the rules of scalar laws enable us to verify without difficulty that this subset of G is stable for the inverse law $\bar{*}$, since, with the obvious notation,

$$(a \perp g) \,\bar{*}\, (b \perp g) = (a - b) \perp g$$

It follows that

$$\operatorname{grp}(g) = \{z \perp g \mid z \in \mathrm{Z}\}$$

We shall put

$$\operatorname{grp}(g) = \{z \perp g \mid z \in \mathrm{Z}\} = \mathrm{Z} \perp g$$

Exercise

Prove that every cyclic group is commutative. (Make use of the formula (Ch. 3. §4.1.))

§11. EXERCISES

1. In a group M, +, the cyclic group of an element is the set of its scalar multiples. In other words:

$$\forall x \in \mathrm{M}: \qquad \operatorname{grp}(x), + \ = \{zx \mid z \in \mathrm{Z}\}, +$$

We shall quite naturally say here again

$$\operatorname{grp}(x) = \{zx \mid z \in \mathrm{Z}\} = \mathrm{Z}x$$

2. In a group H, . the cyclic group of an element is the set of its powers with rational integral exponents.

$$\forall y \in \mathrm{H}: \qquad \mathrm{grp}\,(y), . = \{y^z \mid z \in \mathrm{Z}\}, .$$

3. What is the subgroup generated by 1/2 in $\mathrm{R}_0^+, .$?

4. Compare the following subgroups in $\mathrm{R}_0, .$

$$\mathrm{grp}\,(1);\quad \mathrm{grp}\,(1/2);\quad \mathrm{grp}\,(-1/2);\quad \mathrm{grp}\,(2);\quad \mathrm{grp}\,(-2);$$
$$\mathrm{grp}\,(4);\quad \mathrm{grp}\,(8);\quad \mathrm{grp}\,(-8);\quad \mathrm{R}_0^+, .$$

Show in particular that we have:

$$\mathrm{grp}\,(8) \subset \mathrm{grp}\,(2)$$
$$\mathrm{grp}\,(8) \subset \mathrm{grp}\,(\mathrm{R}_0^+)$$
$$\mathrm{grp}\,(4) \subset \mathrm{grp}\,(-2)$$
$$\mathrm{grp}\,(-8) \cap \mathrm{R}_0^+ = \mathrm{grp}\,(64)$$

5. In $\mathrm{R}_0, .$ find $n \in \omega$ such that

$$\mathrm{grp}\,(-5) \cap \mathrm{R}_0^+ = \mathrm{grp}\,(n)$$

6. In the group R/Z, + define in full the cyclic subgroups

$$\mathrm{grp}\,(0)$$
$$\mathrm{grp}\,(\cdot 5)$$
$$\mathrm{grp}\,(\cdot 1111\ldots)$$

§12. AN EXPRESSION FOR THE SUBGROUP GENERATED BY A SUBSET OF A GROUP

Let G, $*$ be a group and $\mathrm{P} \subset \mathrm{G}$ a non-empty subset. Denote by $\overline{\mathrm{P}}$ the set of symmetrics of the elements of P.
Then

$$\overline{\mathrm{P}} = \{\bar{p} \mid p \in \mathrm{P}\}$$

and we put

$$\mathrm{P}' = \mathrm{P} \cup \overline{\mathrm{P}}$$

Having done this, we are in a position to enunciate the result

$$\mathrm{grp}\,\mathrm{P} = \{p_1' * p_2' * \ldots * p_n' \mid n \in \omega_0; \quad p_1', \ldots, p_n' \in \mathrm{P}'\}$$

In particular, in the case of a group written G, ., grp P is the set of products of factors that are elements of P or inverses of elements of P.

For a commutative group M, + this result may be somewhat

simplified. For this time, as a consequence of commutativity, we can group together all the terms equal to the same $p \in \mathrm{P}$ or to its negative. Finally, grp P appears as the set of linear combinations with rational integral coefficients of a finite number of elements of P:

$$\mathrm{grp}\,\mathrm{P} = \{z_1p_1 + \ldots + z_np_n \mid n \in \omega_0; \quad z_1, \ldots, z_n \in \mathrm{Z}; \quad p_1, \ldots, p_n \in \mathrm{P}\}$$

In the still more restricted case where P is a finite set

$$\{x_1, x_2, \ldots, x_m\}$$

we have

$$\mathrm{grp}\,\mathrm{P} = \mathrm{grp}\,\{x_1, x_2, \ldots, x_m\} = \{z_1x_1 + \ldots + z_mx_m \mid z_1, \ldots, z_m \in \mathrm{Z}\}$$

§13. COSETS, THE ORDER OF A GROUP AND OF A SUBGROUP

Let us consider a group G, $*$ and one of its subgroups H.
For every $g \in \mathrm{G}$, put

$$g * \mathrm{H} = \{g * h \mid h \in \mathrm{H}\} \tag{1}$$

The $g * \mathrm{H}$ are called the left cosets of the subgroups H. We shall show that the set of cosets $\{g * \mathrm{H} \mid g \in \mathrm{G}\}$ is a partition† of G.
Let us first note that we have

$$\forall g \in \mathrm{G}: \qquad g \in g * \mathrm{H}$$

(Since H contains the neutral element ν, and therefore $g = g * \nu \in g * \mathrm{H}$.)
It follows that each of the $g * \mathrm{H} \neq \varnothing$ and that their union is none other than G. In symbols:

$$\cup \{g * \mathrm{H} \mid g \in \mathrm{G}\} = \mathrm{G} \tag{2}$$

which can be written more simply

$$\bigcup_{g \in \mathrm{G}} g * \mathrm{H} = \mathrm{G} \tag{3}$$

It remains to prove that two distinct cosets are disjoint. In other words

$$a * \mathrm{H} \neq b * \mathrm{H} \Rightarrow (a * \mathrm{H}) \cap (b * \mathrm{H}) = \varnothing \tag{4}$$

This is equivalent to proving that

$$(a * \mathrm{H}) \cap (b * \mathrm{H}) \neq \varnothing \Rightarrow a * \mathrm{H} = b * \mathrm{H} \tag{5}$$

† Tr. See Appendix.

In order to do this, let us start by observing that if x is an element of H, we necessarily have

$$x * \mathrm{H} = \{x * h \mid h \in \mathrm{H}\} = \mathrm{H} \tag{6}$$

In fact, since H is stable for $*$ and $x \in \mathrm{H}$, we have

$$x * \mathrm{H} \subset \mathrm{H} \tag{7}$$

On the other hand, let $y \in \mathrm{H}$. Since H, $*$ is a group, the equation

$$x * h = y \tag{8}$$

has a solution $h \in \mathrm{H}$. This proves that

$$\mathrm{H} \subset x * \mathrm{H} \tag{9}$$

Formulae (7) and (9) then give

$$x * \mathrm{H} = \mathrm{H} \tag{6}$$

We are now in a position to establish proposition (5). Since

$$(a * \mathrm{H}) \cap (b * \mathrm{H}) \neq \varnothing$$

there exists an element u such that

$$u \in (a * \mathrm{H}) \cap (b * \mathrm{H}) \tag{10}$$

Since $u \in a * \mathrm{H}$, there exists $h_1 \in \mathrm{H}$ such that

$$u = a * h_1 \tag{11}$$

Similarly, since $u \in b * \mathrm{H}$, there exists $h_2 \in \mathrm{H}$ such that

$$u = b * h_2 \tag{12}$$

Formulae (11) and (12) imply

$$a * h_1 = b * h_2 \tag{13}$$

Whence

$$\bar{a} * b = h_1 * \bar{h}_2 \in \mathrm{H} \tag{14}$$

and finally

$$\bar{a} * b \in \mathrm{H} \tag{15}$$

Applying the preliminary result, we deduce from (15)

$$(\bar{a} * b) * \mathrm{H} = \mathrm{H} \tag{16}$$

From this we obtain successively

$$\begin{aligned} b * \mathrm{H} &= (a * (\bar{a} * b)) * \mathrm{H} && \text{(property of the symmetric of an element)} \\ &= a * ((\bar{a} * b) * \mathrm{H}) && \text{(by the associativity of } *) \\ &= a * \mathrm{H} && \text{(by (16))} \end{aligned}$$

Q.E.D.

We have therefore established that the set of left cosets of H, $\{g * \mathrm{H} \mid g \in \mathrm{G}\}$, is a partition of G.

We shall now prove that left multiplication by g defines a bijection† between any two classes of this partition.

Indeed, let x and $y \in \mathrm{G}$. Since G, $*$ is a group, there exists an element $g \in \mathrm{G}$ such that

$$g * x = y \tag{17}$$

This being so, left multiplication by g defines a map

$$x * \mathrm{H} \to y * \mathrm{H}: \qquad x * h \to y * h = g * x * h$$

whose inverse is none other than the map defined by left multiplication by $\bar{g}$,

$$y * \mathrm{H} \to x * \mathrm{H}: \qquad y * h \to x * h = \bar{g} * y * h$$

Thus left multiplication by g defines a bijection $x * \mathrm{H} \to y * \mathrm{H}$.

We have just shown that all left cosets of a finite group G consist of the same number of elements. Since $\mathrm{H} = \nu * \mathrm{H}$ is one of these cosets, we may conclude that all the cosets have the same number of elements as the subgroup H.

The number of its elements is called the *order* of a finite group, and the number of left cosets which it defines is called the *index* of a subgroup. We can therefore enunciate

Theorem 5 (*Lagrange*) – *The order of a subgroup divides the order of a finite group, and the index of the subgroup* (*or the number of its cosets*) *is the quotient of the order of the group by the order of the subgroup.*

Let H be a subgroup of G, $*$. We know that the set of left cosets of H is a partition of G the number of whose pieces is the index of H and whose every piece contains a number of elements equal to the order of H. We therefore have

$$\text{order of G} = (\text{index of H}) \,.\, (\text{order of H})$$

† Tr. See Appendix.

Exercises

1. What are the cosets of

$$nZ \text{ in } Z, +\ ?$$

Show that there exists a natural bifunction between this set and Z_n.

2. What are the cosets of

$$\text{grp}\left(\frac{4}{8}\right) \text{ in } Z_8\ ?$$

3. What are the cosets of Z, + in R, + ? Establish a bifunction between this set and R/Z.

§14. EXERCISES

1. Show that Z_p, + where p is prime does not contain a non-trivial subgroup.

2. What are the subgroups of Z_{12}, + ?

3. Z_{12}, + is the subgroup of R/Z, + generated by $\frac{1}{12} = \cdot 08333\ldots$.

In general Z_n, + is the subgroup of R/Z, + generated by $\frac{1}{n}$.

4.
$$\begin{aligned} &Z_{12}, + \supset Z_6, + \supset Z_2, + \supset \{0\}, + \\ &Z_{12}, + \supset Z_6, + \supset Z_3, + \supset \{0\}, + \\ &Z_{12}, + \supset Z_4, + \supset Z_2, + \supset \{0\}, + \end{aligned}$$

Establish that the inclusion chains of subgroups given above are maximal in the sense that there do not exist subgroups which lie strictly between two successive subgroups. For example

$$Z_6 \supset G \supset Z_2 \Rightarrow Z_6 = G \quad \text{or} \quad G = Z_2$$

5. Let z denote a rational integer (i.e. $z \in Z$).

(a) In the case of the subgroup $2Z = Z2$ generated by the element 2 in the group Z, + we have

$$z2 = 0 \Leftrightarrow z = 0$$

(b) Show that this is not so in the case of the subgroup generated by $\frac{1}{3}$ in the group R/Z, +. (We recall that by $\frac{1}{3}$ we mean "1/3 modulo 1".) ($z \cdot \frac{1}{3} = 0$ does not necessarily imply that $z = 0$.)

(c) Show that in the subgroup generated by "$\sqrt{2}$ modulo 1" in R/Z, + we have again

$$z(\sqrt{2} \text{ modulo } 1) = 0 \Leftrightarrow z = 0$$

6. For every $b \in \omega_0$, the set $\{z/b^n \} z \in Z, n \in \omega\}$ is a subgroup of Q, +, and $L_b = \left\{\frac{z}{b^n}\right\} z \in Z, n \in \omega\}$ is a subgroup of R/Z which is fundamental in the theory of commutative groups.

If p is prime, all the proper subgroups of the infinite group L_p are finite. (If there is any difficulty, consult the revision exercises on the entire book, p. 195, Ex. 1.)

Revision exercises on Chapter 4

1. Find subgroups of C, +.
2. Find subgroups of C_0, ..
3. Is the subset 2Z of Z a subgroup of Z, + ?
4. The same question for nZ with $n \in \omega_0$.
5. The same question for ω.
6. Is the subset 2Z + 1 of Z a subgroup of Z, + ?
7. Is the subset 2Z + 1 of Q a subgroup of Q, + ?
8. Is the subset 2Z + 1 of Q_0 a subgroup of Q_0, . ?
9. Q_0^+, . is a subgroup of Q_0, ..
10. $\{1, -1\}$ is a subgroup of Q_0, ..
11. Prove that $\{1, -1, i, -i\}$, . is a subgroup of the quaternion group (see revision exercises on chapters, 1, 2, exercise 41, d).
12. Let M be provided with an associative law $*$ and with a neuter. Prove that the set of symmetrizable elements is a stable subset of M, $*$.
13. What is the stable subset of Z, + generated by 3 ?
What is the stable subset of Z, − generated by 3 ?
What is the stable subset of ω, + generated by 3 ?
What is the stable subset of ω, . generated by 3 ?
What is the stable subset of Z, + generated by 1 ?
14. The stable subset of ω, + generated by 1 is ω_0.
The stable subset of ω, . generated by 1 is $\{1\}$.
15. Let E possess a law $*$. Let $s \in E$.
We have:

$\{s\}$ is a stable subset of E, $* \Leftrightarrow s$ is idempotent.

16. What is the subgroup of Z, + generated by 1?
What is the subgroup of Z, + generated by 2?
What is the subgroup of Z, + generated by -2?
What is the subgroup of Z, + generated by -9999?

17. If every element of a generating subset of a group commutes with all the other elements of this generating subset, the group is commutative.

18. Let us consider the symmetric group of $\{1, 2, 3, 4, 5\}$, i.e. the group of permutations of $\{1, 2, 3, 4, 5\}$. We denote it by $\mathscr{S}_5$.
What is the subgroup generated in $\mathscr{S}_5$, $\circ$ by

$$\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}?\dagger$$

What is the subgroup generated by the set of permutations

$$\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix} \text{ and } \begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}?\dagger$$

What is the subgroup generated by the set of three permutations

$$\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix}, \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}, \begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}?\dagger$$

19. What is the subgroup of the quaternion group generated by the subset $\{i, j\}$?
What is the subgroup of the quaternion group generated by the subset $\{1, -1, i, -i\}$?

20. Let the group $R_0 \times R$, . have its multiplication defined by

$$\forall (a, b), (c, d) \in R_0 \times R: \qquad (a, b) \,.\, (c, d) = (ac, bc + d)$$

Prove that the elements $(1, b)$ form a subgroup of $R_0 \times R$.

21. What are the subgroups of the symmetric group of $\{1, 2, 3\}$?

22. What are the subgroups of $\mathscr{S}_4$ (the symmetric group of $\{1, 2, 3, 4\}$)?

What is the subgroup of $\mathscr{S}_4$ generated by $\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}?\dagger$

What is the subgroup of $\mathscr{S}_4$ generated by $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}?\dagger$

† For the notation see Ch. 8, §1.

What is the subgroup of $\mathscr{S}_4$ generated by

$$\left\{\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}\right\}?\dagger$$

23. What are the subgroups of Z_{12}? For each subgroup give a generating subset.

24. The set of permutations (1 2), (3 4), (1 3) $\circ$ (2 4)† of $\{1, 2, 3, 4\}$ generates a group of what order?

25. The permutation (1 2 3 4) generates a group of order 4.†

26. The permutation (1 2 3 4) $\circ$ (5 6 7 8) $\circ$ (9 10 11 12) of $(1, 2, \ldots, 12\}$† generates a group of order 4.

27. The permutation $(a_1\, a_2 \ldots a_n)$ generates a group of what order?

28. The permutation $(a_1\, a_2 \ldots a_{n-1} a_n) \circ (a_{n+1} a_{n+2} \ldots a_{2n-1} a_{2n}) \circ \ldots \circ (a_{(q-1)n+1} a_{(q-1)n+2} \ldots a_{qn-1} a_{qn})$ of $\{a_1, a_2, \ldots a_{qn}\}$ generates a group of what order?†

29. What is the order of the group generated by

$$\{(1\ 2\ 3\ 4), (5\ 6\ 7\ 8), (9\ 10\ 11\ 12)\} \text{ in } \mathscr{S}_{12}?\dagger$$

30. What is the order of the group generated by the subset

$$\{(a_1 a_2 \ldots a_{n-1} a_n), (a_{n+1} a_{n+2} \ldots a_{2n-1} a_{2n}), \ldots, (a_{(q-1)n+1} a_{(q-1)n+2} \ldots a_{qn-1} a_{qn})\}$$

of $\mathscr{S}\{a_1, \ldots a_{qn}\}$?

31. Prove that for every $n \in \omega_0$, there exists a cyclic group of order n.

32. Every subgroup of a cyclic group is cyclic.

33. What is the subgroup of the cyclic group Z_{24}, + generated by $\frac{3}{24}$?

What is the subgroup of Z_{24}, + generated by $\frac{5}{24}$?

34. What is the subgroup of the cyclic group Z_{13}, + generated by $\frac{3}{13}$? by $\frac{5}{13}$? by $\frac{10}{13}$?

35. A group of prime order admits only trivial subgroups as subgroups.

† For the notation see Ch. 8, §1.

36. By the *order of* g belonging to the group G, $*$ we mean the order of the subgroup generated by g.

If g is of finite order, prove that the order of g is the smallest $n \in \omega_0$, such that $n \perp g = \nu$.

37. The order of every element of the finite group G, $*$ divides the order of this group G.

38. In every group the neuter is the only element of order 1.

39. Every group in which all the elements except the neuter are of order 2 is commutative.

40. Every group of prime order p is cyclic and the order of every element different from the neuter is p.

41. Let $a \in G, +$. If grp (a) is of order $n < \infty$, then grp (ma) is of order $(m \vee n)/m = n/(m \wedge n)$.

42. The order of a permutation is the L.C.M. of the orders of the disjoint cycles of which it is the product (see exercises 29, 30).

43. Let g be an element of G, $+$. If the order of g is n, then $(mg = 0 \Leftrightarrow n/m)$.

44. If G_1 and G_2 are finite subgroups of a group G such that $\# G_1 \wedge \# G_2 = 1$, we have $\# (G_1 \cap G_2) = 1$†.

45. Partition the quaternion group $\mathcal{Q}, .$ into left cosets with respect to the subgroup generated by i.

What are the cosets of grp (j), of grp (k), of grp (1), of grp (-1) and of grp $\{i, j\}$ (each time in $\mathcal{Q}, .$)?

46. Denote the symmetric group of $\{1, 2, 3\}$ by $\mathcal{S}_3$. Find the cosets of $\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\}$ in $\mathcal{S}_3$.

47. What are the cosets of grp (a) in Klein's four-group? The same question for grp (b), grp $(a * b)$ and grp $\{a, b\}$ (each time in V)?

48. Denote the symmetric group of $\{1, 2, 3, 4\}$ by $\mathcal{S}_4$. Denote by V the subgroup $\left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$ of $\mathcal{S}_4$. Find the cosets of V in $\mathcal{S}_4$.

49. If H is a subgroup of the group G, $*$

$$\forall g \in G: \quad g * H = H \Leftrightarrow g \in H$$
$$\forall a, b \in G: \quad a * H = b * H \Leftrightarrow \bar{a} * b \in H \Leftrightarrow \bar{b} * a \in H$$
$$\forall a, b \in G: \quad H * a = H * b \Leftrightarrow b * \bar{a} \in H \Leftrightarrow a * \bar{b} \in H.$$

† Tr. See Appendix.

5

Modules or Commutative Groups

§1. INTERSECTION OF SUBMODULES

Let M, $+$ be a module or a commutative group whose law is denoted $+$. Its subgroups are called sub-modules or simply modules, and we shall denote by mod P the submodule of M, $+$ generated by the subset P of M.

The set $\mathfrak{M}$ of submodules of M, $+$ is ordered by inclusion and is stable for the law $\cap$. The intersection $A \cap B$ of two submodules of M, $+$ is the largest submodule of M which is smaller than A and smaller than B. We express this fact by saying that $A \cap B$ is the *infimum* of A and B in the (partially) ordered set $\mathfrak{M}, \subset$.

In symbols:

$$\forall A, B \in \mathfrak{M}: \qquad A \cap B = \inf \{A, B\}$$

Exercises

1. We recall that a relation defined in a set E is called an *ordering*§ when it is at the same time reflexive, transitive and anti-symmetric†.

Every set E provided with an ordering is called an *ordered* set.

Let $\prec$ be an ordering defined in the set E. (If $a \prec b$ we shall say that a is smaller than b.)

We have defined implicitly above the infimum (when it exists) of two elements of the ordered set T, $\prec$.

We define the infimum of $\{a, b\} \subset T$ to be the largest element of T which is simultaneously smaller than a and b.

In the ordered set

$$(\omega \setminus \{0, 1\}), |‡$$

the pair $\{2, 3\}$ has no infimum.

2. In the ordered set $\mathcal{G}, \subset$ of subgroups of the group G, $*$ we have

$$\forall A, B \in \mathcal{G}: \qquad A \cap B = \inf \{A, B\}$$

§2. PRODUCT OF SUBGROUPS OF A GROUP G, $*$

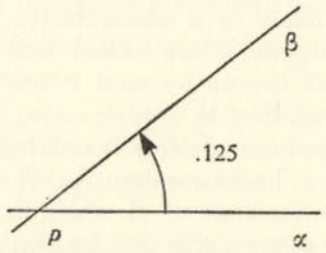
Proposition. The product $A * B = \{a * b \mid a \in A, b \in B\}$ *of the subgroups* A, B *of a group* G, $*$ *is not necessarily a subgroup of* G, $*$.

† Tr. See Appendix. ‡ Tr. See Ch. 6 §5.

§ Tr. This is sometimes called a partial ordering. See Appendix.

Consider the group G, $\circ$ formed by the plane rotations with centre p and the symmetries with respect to straight lines containing the point p. Let I be the identical transformation and denote by a and b the symmetries with respect to the straight lines α and β (see figure).

It is evident that $A = \{I, a\}$ and $B = \{I, b\}$ are subgroups of G, $\circ$.



It then follows that

$$B \circ A = \{I, a, b, b \circ a = r\}$$

where $r = b \circ a = \text{rot}\,(p\,;\,\cdot 25)$.
(where rot $(p\,;\,\cdot 25)$ denotes the rotation with centre p and of angle $\cdot 25$ grades).†

Consequently $r^2 = r \circ r = \text{rot}\,(p\,;\,\cdot 5)$
$= \text{a symmetry with respect to } p,$

whence $r^2 \notin B \circ A$ and $B \circ A$ is not a subgroup of G, $\circ$.

§3. ADDITION OF SUBMODULES

Proposition. The sum $A + B = \{a + b \mid a \in A, b \in B\}$ *of the submodules* A *and* B *of* M, + *is a submodule of* M, +. *Furthermore, in the ordered set* $\mathfrak{M}$, $\subset$ *of the submodules of* M, + *we have*

$$\forall A, B \in \mathfrak{M}: \qquad A + B = \sup\{A, B\}$$

By the last equality we are claiming that A + B is the *supremum* of A and B, i.e. the smallest of the elements of $\mathfrak{M}$, $\subset$ which are larger than A and B. This is an immediate consequence of the first part of the proposition.

To establish that A + B is a submodule of M, + it is sufficient to prove that the difference of two elements of A + B belongs to A + B.

† Tr. Here we have 1 grade = 1 revolution = 360°.

Let $a_1, a_2 \in A$ and $b_1, b_2 \in B$.
Then $a_1 + b_1 \in A + B$ and $a_2 + b_2 \in A + B$.
We get

$$\begin{aligned}(a_1 + b_1) - (a_2 + b_2) &= (a_1 + b_1 - b_2 - a_2) && \text{(general properties of groups)}\\ &= (a_1 - a_2) + (b_1 - b_2) && \text{(associativity and commutativity of +)}\\ &\in A + B\end{aligned}$$

Q.E.D.

Exercises

1. In R, $\leqslant$

$$\inf\{5, \sqrt{2}\} = \sqrt{2}; \qquad \sup\{5, \sqrt{2}\} = 5$$

2. In ω, $|$

$$\inf(12, 16) = 4; \qquad \sup(12, 16) = 48$$

3. In the ordered set $\mathscr{G}$, $\subset$ of subgroups of the group G, $*$ we have

$$\forall A, B \in \mathscr{G}: \qquad \sup\{A, B\} = \text{grp}\,(A \cup B)$$

4. In the ordered set $\mathfrak{M}$, $\subset$ of submodules of the module M, + we have

$$\forall A, B \in \mathfrak{M}: \qquad A + B = \sup\{A, B\} = \text{mod}\,(A \cup B)$$

§4. LATTICES

Every ordered set in which every pair of elements admits an infimum and a supremum is called a *lattice*.

Examples

1. Every totally ordered set† is a lattice.
2. ω, $|$ is a lattice $(\inf\{a, b\} = a \wedge b; \quad \sup\{a, b\} = a \vee b)$
3. For every set E, the ordered set $\mathscr{P}E$, $\subset$ is a lattice

$$\inf\{A, B\} = A \cap B; \qquad \sup\{A, B\} = A \cup B$$

4. The set $\mathscr{G}$ of subgroups of a group G ordered by inclusion is a lattice

$$\inf\{A, B\} = A \cap B; \qquad \sup\{A, B\} = \text{grp}\,(A \cup B)$$

† Tr. See Appendix.

Note in particular that the set $\mathfrak{M}$ of subgroups of a module M, + is a lattice (for inclusion).

We have

$$\inf\{A, B\} = A \cap B; \qquad \sup\{A, B\} = A + B$$

5. If A and B are subsets of the module M, + we have

$$\operatorname{mod} A + \operatorname{mod} B = \operatorname{mod}(A \cup B)$$

In particular, we have

$$\operatorname{mod}\{a, b\} = \operatorname{mod} a + \operatorname{mod} b$$
$$\operatorname{mod}\{a, b, \ldots, m\} = \operatorname{mod} a + \operatorname{mod} b + \ldots + \operatorname{mod} m$$

§5. EXERCISE

The set V of vectors of ordinary space having a point 0 as origin is a module for the addition of vectors. If Δ is a straight line passing through 0, the set of vectors of V with their end-points in Δ is a submodule of V.

Let α be a plane containing the point 0. The set of vectors of V with their end-points in α is a submodule of V.

Let A, B, C be submodules of V defined by three non-coplanar straight lines each containing 0. The reader is asked to describe the submodules A + B, B + C, C + A.

Establish the equalities

$$A \cap B = B \cap C = C \cap A = \{0\}$$
$$(A + B) \cap (B + C) = B$$
$$(B + C) \cap (C + A) = C$$
$$(C + A) \cap (A + B) = A$$
$$A + B + C = V$$
$$(A + B) \cap (B + C) \cap (C + A) = \{0\}$$

Let X and Y be submodules defined by new straight lines containing 0. Knowing that $X \neq Y$ and $A + B \neq X + Y$ what can you say about

$$(A + B) \cap (X + Y)?$$

§6. DEDEKIND'S THEOREM

Lattices are provided with two inner laws, the infimum and the supremum.

We know that, in the case of a lattice $\mathscr{P}E$, $\subset$, $\cap$, $\cup$ we have the double distributivity

$$\forall A, B, C \in \mathscr{P}E: \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

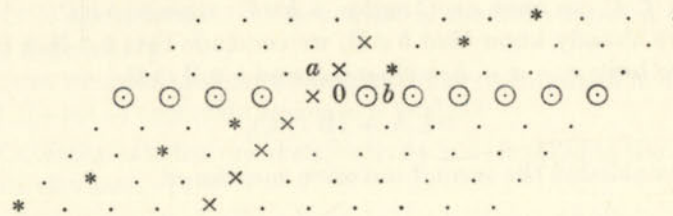
The lattice $\mathfrak{M}$, $\subset$ of submodules of a module M, + does not (in general) satisfy either of these rules.

Counter-example

Let a and b be two non-collinear vectors with the same origin 0. Consider the module W, + defined by

$$W = Za + Zb$$

Since all the vectors we have to consider have the same origin 0, it is convenient to denote them by their extremities. This being so, the points of the figure below represent vectors of the module W, +; in particular the vectors of Za and Zb are represented respectively by crosses and small circles and the vectors of $Z(a + b)$ are represented by stars



It follows that

$$Z(a + b) \cap (Za + Zb) = Z(a + b) \cap W = Z(a + b)$$
$$(Z(a + b) \cap Za) + (Z(a + b) \cap Zb) = \{0\} + \{0\} = \{0\}$$
$$Z(a + b) + (Za \cap Zb) = Z(a + b) + \{0\} = Z(a + b)$$
$$(Z(a + b) + Za) \cap (Z(a + b) + Zb) = W \cap W = W$$

Thus we have just seen that the set of submodules of W, + does not satisfy either of the two rules of distributivity.

We shall establish that in every module M, +, three submodules A, B and C satisfy the distributivity rule of + with respect to $\cap$ as long as $A \subset C$. More precisely, we shall prove that if A, B, C are submodules of any module:

$$A \subset C \Rightarrow A + (B \cap C) = (A + B) \cap (A + C)$$

Since $A \subset C \Rightarrow A + C = C$, we have to establish

Dedekind's modular theorem – If A, B, C are submodules of any module,

$$A \subset C \Rightarrow A + (B \cap C) = (A + B) \cap C$$

Proof

We shall show successively that we have

$$A + (B \cap C) \subset (A + B) \cap C$$

and

$$(A + B) \cap C \subset A + (B \cap C)$$

1. Let $x \in A + (B \cap C)$;

then $x = a + d$, with $a \in A$, $d \in B \cap C$.
Since $d \in B$, $x = a + d \in A + B$.
Since $d \in C$, then $x = a + d \in A + C$.
Therefore $x \in (A + B) \cap (A + C) = (A + B) \cap C$, which establishes our first inclusion.

2. Let $x \in (A + B) \cap C$;

whence $x = a + b$, with $a \in A$ and $b \in B$ and $a + b \in C$.
Since $A \subset C$, we have $a \in C$ and $a + b \in C$; whence $b \in C$.
Since we already know that $b \in B$, we conclude that $b \in B \cap C$.
Thus we have $x = a + b$, with $a \in A$ and $b \in B \cap C$,

hence

$$x \in A + (B \cap C),$$

which establishes the second inclusion mentioned.

Exercise

If A, B, C are submodules of any module, we always have

$$A \cap (B + C) \supset (A \cap B) + (A \cap C)$$

and

$$A + (B \cap C) \subset (A + B) \cap (A + C)$$

Note

Let A, B, C be submodules of any module whatsoever. We have already seen that if we apply the distributivity rule of $+$ with respect to $\cap$ to the expression $A + (B \cap C)$ knowing that $A \subset C$, we find that

$$A + (B \cap C) = (A + B) \cap C$$

It is interesting to note that if we apply the distributivity rule of

$\cap$ with respect to $+$ to the expression $(A + B) \cap C$ knowing that $A \subset C$, we find that

$$\begin{aligned}(A + B) \cap C &= (A \cap C) + (B \cap C) \\ &= A + (B \cap C)\end{aligned}$$

Thus the modular rule appears to be the expression of an attenuated (or conditional) distributivity both for the law $+$ with respect to the law $\cap$ and for the law $\cap$ with respect to the law $+$.

Revision exercises on Chapter 5

1. We have seen (§3) that the sum $A + B$ of two submodules A and B is a submodule. This property can be generalized: prove that if A and B are two subgroups of the group G, $*$, the product $A * B$ is a subgroup of G, $*$ if and only if $A * B = B * A$.

2. Denote by $\mathscr{S}$ the set of segments of a straight line D; (we recall that for every $(a, b) \in D \times D$ such that $a \leqslant b$, the segment

$$[a, b] \text{ is defined by } [a, b] = \{x \in D \mid a \leqslant x \leqslant b\})$$

$\mathscr{S}$ is ordered by inclusion. The reader is asked to show that $\mathscr{S}$, $\subset$, $\cap$, $\cup$ is not a lattice. (Clue: what is the infimum of a pair of disjoint segments?)

How can we make a slight alteration in the definition of a segment so that the set of segments becomes a lattice?

3. If a lattice satisfies one distributivity law, it satisfies the double distributivity law.

4. In how many distinct ways can we make a set of 3 elements into a lattice? (It is advisable to use diagrams.)

5. The same problem for a set comprising 4 elements.

6. Let E be a set of 5 elements. Define two orderings $\leqslant_1$ and $\leqslant_2$ on E such that E, $\leqslant_1$, inf, sup is a lattice and E, $\leqslant_2$, inf, sup is not a lattice.

6

The group Z, +

§1. We have already cited the group Z, + as an example and we have used when necessary some of its properties when we defined the scalar law. We shall recall these properties below, and, using the ideas of group theory, we shall undertake a detailed study of Z, + which will lead onto the fundamental theorems of elementary arithmetic.

§2. FUNDAMENTAL PROPERTIES OF Z, +, ⩽

Z is the set of rational integers and may be defined starting from the set ω of natural integers

$$\omega = \{0, 1, 2, 3, \ldots\}$$

The elements of ω are the cardinals of finite sets. The number 0 is the cardinal of the empty set; the number 1 is the cardinal of every set comprising a single object.

The set ω is furnished with an inner law named addition and defined in the theory of sets. This law is everywhere defined, associative and commutative and it admits the neutral element 0.

For every $n \in \omega_0$, the number n is the sum of n terms equal to 1.

$$n = \underbrace{1 + 1 + \ldots + 1}_{n \text{ terms}}$$

This law admits cancellation, i.e.

$$\forall a, x, y \in \omega: \qquad a + x = a + y \Rightarrow x = y$$

If $b = a + x$, with $a, b, x \in \omega$, we write

$$a \leqslant b$$

and we write

$$a < b$$

if we know that $a \neq b$.

From the cancellation property, the element x is completely defined by the pair (a, b) and we write

$$x = b - a$$

Thus there is defined in ω an inner law denoted by $-$ and called subtraction.

If x and y are two elements of ω, we have $x \leqslant y$ or $y \leqslant x$.

Since the union of non-empty sets is a non-empty set, every sum of non-null elements of ω is not null. It follows that the null element of ω is the only element of ω which admits a symmetric in ω.

Consequently to extend ω, + to a group it is necessary to add to ω some new elements as symmetrics of the elements of ω_0. We do this by putting

$$\mathrm{Z} = (-\omega_0) \cup \omega$$
$$-\omega_0 = \{-n \mid n \in \omega_0\}$$

Evidently we assume $\omega \cap (-\omega_0) = \varnothing$, and since in a group two distinct elements have distinct symmetrics, the map $\omega_0 \to -\omega_0 : n \to -n$ must be a bifunction.

We know that in any group,

$$-(x + y) = -y - x$$
(by putting $-y - x = -y + (-x)$)

We therefore must put

$$\forall x, y \in \omega: \qquad (-x) + (-y) = -(y + x) = -(x + y)$$

Thus $-\omega_0$ possesses a commutative and associative addition. It remains to define the sum

$$x + (-y) \quad \text{with} \quad x, y \in \omega_0$$

We know that we have

$$y \leqslant x \quad \text{or} \quad x \leqslant y$$

If $y \leqslant x$, let us put

$$x + (-y) = x - y$$

and if $x \leqslant y$,

$$x + (-y) = -(y - x)$$

Thus Z is provided with a law + everywhere defined, and the

reader can establish without difficulty that Z, + is a commutative group.

We already know that ω is a stable subset of Z for addition. We shall say in general

$$\forall x, y \in \mathrm{Z}: \qquad x \leqslant y \Leftrightarrow y - x \in \omega$$

The relation $\leqslant$ defines an ordering in Z. Since $\mathrm{Z} = \omega \cup (-\omega)$, we necessarily have

$$\forall z \in \mathrm{Z}: \qquad z \in \omega \quad \text{or} \quad z \in -\omega$$

Therefore

$$\forall x, y \in \mathrm{Z}: \qquad x \leqslant y \quad \text{or} \quad y \leqslant x$$

We express this property by saying that the ordering $\leqslant$ in Z is *total*, i.e. given any two elements x, y in Z, then either $x \leqslant y$ or $y \leqslant x$.

The law + and the relation $\leqslant$ defined in Z are compatible in the sense that

$$\forall a, b, x, y \in \mathrm{Z}: \qquad a \leqslant b \quad \text{and} \quad x \leqslant y \Rightarrow a + x \leqslant b + y$$

We express this fact by saying that Z, + is an ordered group.

Exercises

1. $\forall x, y \in \mathrm{Z}: \quad x \leqslant y \Leftrightarrow -y \leqslant -x$

In the following work we shall also make use of the fact that every non-empty set of natural integers contains an element $\leqslant$ every element of this set.

2. Prove the different propositions enunciated in the above paragraph.

§3. DEFINITION OF MULTIPLICATION IN Z, +

Since Z, + is a group there is defined a scalar law (Chapter 3, §7)

$$\mathrm{Z} \times \mathrm{Z} \to \mathrm{Z}: \qquad (z, g) \to z \,.\, g$$

Note that this scalar law is here an inner law of Z. We call it multiplication. Let us show that it is commutative.

Proof

By virtue of the properties of the scalar law, we have

$$(-a) \,.\, b = a \,.\, (-b) = -(ab)$$

whence $$(-a)(-b) = a \,.\, b$$

It is therefore sufficient to establish that

$$a \,.\, b = b \,.\, a \quad \text{with} \quad a, b \in \omega$$

Since we evidently have

$$a \,.\, 0 = 0 \,.\, a = 0$$

we may assume $$a, b \in \omega_0$$

Then

$$ab = \underbrace{b + b + \ldots + b}_{a \text{ terms}} \qquad \text{(definition of the scalar law)}$$

$$= \underbrace{\underbrace{(1 + \ldots + 1)}_{b \text{ terms}} + \ldots + \underbrace{(1 + \ldots + 1)}_{b \text{ terms}}}_{a \text{ brackets}} \qquad \text{(definition of } b\text{)}$$

$$= \underbrace{\underbrace{(1 + \ldots + 1)}_{a \text{ terms}} + \ldots + \underbrace{(1 + \ldots + 1)}_{a \text{ terms}}}_{b \text{ brackets}} \qquad \text{(general associativity of + in } \omega_0\text{)}$$

$$= \underbrace{a + \ldots + a}_{b \text{ terms}} \qquad \text{(definition of } a\text{)}$$

$$= ba \qquad \text{(definition of the scalar law)}$$

Q.E.D.

From the general properties of the scalar law the reader should prove moreover that multiplication in Z is associative.

Exercises

1. Prove the associativity of Z, ..
2. $\forall a, b \in \mathrm{Z}: \quad a \,.\, b = 0 \Leftrightarrow a \text{ or } b = 0.$

We note that the rules of scalar laws

$$(b + c)a = ba + ca$$

and $$a(b + c) = ab + ac$$

can each be deduced from the other by commutativity. We say that multiplication in Z is distributive with respect to addition.

Definition. Instead of saying that the module Z, + *is provided with a multiplication written . everywhere defined, associative, and distributive with respect to addition, we shall simply say that* Z, +, . *is a ring.*

We indicate that the multiplication is commutative by saying that the ring Z, +, . is commutative.

Let us now give an explicit definition of a ring which has been defined implicitly above.

Definition. Every module provided with a second inner law, everywhere defined, associative and distributive with respect to addition is called a ring. This second law is called multiplication.

§4. THE ORDERED RING Z, +, ., ⩽

We have seen that Z, +, . is a ring and Z, +, ⩽ an ordered module. We know that ω is the set of positive elements of Z (i.e. elements $\geqslant 0$) and that ω is stable for addition.

It is clear that ω is stable for multiplication. When the module A, + of a ring A, +, . is a module ordered by an ordering ⩽ and the set of positive elements of A is stable for multiplication, we say that A, +, ., ⩽ is an *ordered ring.*

Theorem. Z, +, ., ⩽ *is an ordered ring.*

Corollary. If $a, b, c \in Z$

$$a \geqslant 0 \text{ and } b \leqslant c \Rightarrow ab \leqslant ac$$

The formula $b \leqslant c$ means that $c - b \in \omega$.

Similarly $a \geqslant 0$ is equivalent to $a \in \omega$.

The stability of ω for multiplication implies

$$a(c - b) \in \omega$$

hence also

$$ac - ab \in \omega$$

and

$$ab \leqslant ac$$

Q.E.D.

Exercises

1. Let $a, b, c \in Z$. Establish the result

$$a \leqslant 0 \quad \text{and} \quad b \leqslant c \Rightarrow ab \geqslant ac$$

2. Define $|a|$† and prove the formula

$$||a| - |b|| \leqslant |a + b| \leqslant |a| + |b|$$

3. Let E be a set. Prove that $\mathscr{P}E, \triangle, \cap$ is a ring.

4. Prove that the structures Z, +, . ; Q, +, . ; R, +, . ; C, +, . are rings.

5. Prove that the structure ω, +, . is not a ring.

§5. STUDY OF Z, . . FACTORIZATION

Divisors

We shall say that $a \in Z$ divides $b \in Z$, and we write $a|b$ if and only if there exists a $q \in Z$ such that $b = aq$.

In symbols

$$\forall a, b \in Z: \quad a|b \Leftrightarrow \exists q \in Z: \quad b = aq$$

Instead of saying that a divides b, we can say that a is a divisor (or factor) of b or that b is a multiple of a. We sometimes write $a|b|c$ for $a|b$ and $b|c$.

Exercises

1. $\forall a, b \in Z: \quad a|b \Leftrightarrow a|(-b) \Leftrightarrow (-a)|b \Leftrightarrow (-a)|(-b)$

$$a|b \Leftrightarrow |a| \mid |b|$$

$$a|b \quad \text{and} \quad b|a \Leftrightarrow |a| = |b|$$

$$1|a|(-a)|0$$

$$a|a$$

2. $\forall a, b, c \in Z: \quad a|b|c \Rightarrow a|c$

$$a|b \text{ and } a|c \Rightarrow a|(b + c)$$

3. $\forall a, b, c, m, n \in Z: \quad a|b \text{ and } a|c \Rightarrow a|mb + nc$

$$a|b \Rightarrow a|bc$$

4. The relation | defined in Z is reflexive, transitive but not anti-symmetric: it is not an ordering.

5. The relation | defined in ω is an ordering.
(for the relation | is anti-symmetric in ω

$$a|b \quad \text{and} \quad b|a \Leftrightarrow a = b)$$

† Tr. $|a|$ is the modulus of a, defined by

$$|a| = a, \; a \geqslant 0$$
$$|-a| = a, \; a > 0$$

Non-trivial divisors

Let us denote the set of divisors of z by div z.
In symbols:

$$\operatorname{div} z = \{x \in \mathrm{Z} \mid x|z\}$$

We therefore have

$$\{1, -1, z, -z\} \subset \operatorname{div} z$$

The elements $1, -1, z, -z$ are called the trivial divisors of z.

Exercises

1. $\operatorname{div} 0 = \mathrm{Z}$, $\operatorname{div} 1 = \operatorname{div}(-1) = \{1, -1\}$, $\operatorname{div} z = \operatorname{div}(-z) = \operatorname{div}|z|$.
2. $\operatorname{div} 3 = \{\ldots\}$
   $\operatorname{div} 7 = \{\ldots\}$
   $\operatorname{div} 12 = \{\ldots\}$
   $\operatorname{div}(-18) = \{\ldots\}$
   $\operatorname{div}(4) = \{\ldots\}$
   $\operatorname{div}(8) = \{\ldots\}$
3. $\forall z \in \mathrm{Z}: z \in \operatorname{div} z,\ -z \in \operatorname{div} z,\ |z| \in \operatorname{div} z,\ 1 \in \operatorname{div} z,\ -1 \in \operatorname{div} z.$
4. $a|b \Leftrightarrow \operatorname{div} a \subset \operatorname{div} b \Leftrightarrow a \in \operatorname{div} b$
   $\Leftrightarrow \operatorname{div} a \cap \operatorname{div} b = \operatorname{div} a \Leftrightarrow \operatorname{div} a \cup \operatorname{div} b = \operatorname{div} b$
   $\Leftrightarrow \operatorname{div} a \setminus \operatorname{div} b = \varnothing$
5. $\operatorname{div} x = \operatorname{div} y \Leftrightarrow |x| = |y|$.

Proposition 1

$$\forall a, b \in \mathrm{Z}_0: \quad a|b \Rightarrow |a| \leqslant |b| \tag{1}$$

If a is a non-trivial divisor of b, we have

$$|a| < |b| \tag{2}$$

Proof

The statement $a|b$ is equivalent to $|a| \mid |b|$.
If $a|b$ then there exists an $m \in \omega_0$ such that $|b| = m \cdot |a|$.
If $m = 1$, (1) is verified.
If $m \neq 1$, we have

$$|b| = |a| + (m-1)|a| \qquad (m-1) \in \omega$$

Hence

$$|b| - |a| \in \omega \quad \text{and} \quad |a| \leqslant |b|$$

If a is a non-trivial divisor of b, we have $(m-1) \in \omega_0$, hence (2).

Corollary

For every $z \in \mathrm{Z}_0$, a chain of successive non-trivial divisors

$$\ldots |d_5|d_4|d_3|d_2|d_1|z$$

is necessarily finite.
In fact we have in this case

$$|z| > |d_1| > |d_2| > \ldots$$

Invertible elements

An element x of Z is said to be invertible if and only if there exists $x' \in \mathrm{Z}$ such that $xx' = 1$. It is easy to see that x is invertible $\Leftrightarrow -x$ is invertible $\Leftrightarrow |x|$ is invertible, and that the only invertible elements of Z are the numbers 1 and -1. (If $a, b \in \omega_0$ and a or $b \neq 1$, we have $ab \neq 1$.)

Prime numbers

An element p of Z is said to be prime if and only if it is not invertible and if its only divisors are its trivial divisors.

$$p \text{ prime} \Leftrightarrow \begin{cases} p \text{ is not invertible in Z} \\ \operatorname{div} p = \{1, -1, p, -p\} \end{cases}$$

Exercises

1. The number 2 is prime.
2. p prime $\Leftrightarrow -p$ prime $\Leftrightarrow |p|$ prime.

Proposition 2. *Every non-invertible rational integer admits a positive prime divisor.*

Let z be a non-invertible rational integer.
If $z = 0$ the proposition is obvious since $2|0$.
Let D be the set of non-invertible divisors of z.
Then $\mathrm{D} = \operatorname{div} z \setminus \{1, -1\}$.
Since z is not invertible we have $\mathrm{D} \neq \varnothing$.
Moreover $d \in \mathrm{D} \Rightarrow |d| \in \mathrm{D}$.
Therefore $\mathrm{D} \cap \omega \neq \varnothing$.
Let p be the minimum (i.e. the smallest element) of $\mathrm{D} \cap \omega$ (for the usual ordering $\leqslant$).
We shall show that p is prime.
Let d be a non-invertible divisor of p.

Then $1 \neq |d| \mid p$.
We have $|d| \leqslant p$ and $|d| \in \mathrm{D} \cap \omega$.
Therefore $|d| = p$ and p is prime.

Q.E.D.

Proposition 3. *Every rational integer which is neither null nor invertible is the product of prime integers.*

Once again we consider every number to be the product of itself alone. Thus a prime number is "the product" of this sole prime number. And the proposition is true for the prime integers.

Let z be a rational integer, neither null nor invertible. It is clear that z will be a product of primes if and only if this is true of $|z|$. It is therefore sufficient to prove that $|z|$ is a product of primes.

If z is prime the proposition is proved. Assume z is not prime.

From the preceding proposition, there exists a positive prime p_1 such that $p_1 \mid |z|$.

We therefore have $|z| = p_1 q_2$ where q_2 is a natural integer which is neither null nor invertible. If q_2 is prime the proposition is verified. (We then write p_2 instead of q_2.)

If q_2 is not prime, there exists a positive prime p_2 which divides q_2. We then have $q_2 = p_2 q_3$ where q_3 is, in its turn, a natural integer which is neither null nor invertible.

If q_3 is prime the proposition is verified (and we then write p_3 instead of q_3). Etc. . . .

If at the end of a finite number of steps we find a prime quotient q_n, (we then put $p_n = q_n$) we obtain the prime factorization $|z| = p_1 \cdots p_n$.

It therefore remains to prove that after a certain finite number of steps we necessarily find a prime quotient.

If this were not the case we would have an unlimited sequence of positive proper divisors

$$\ldots \mid q_7 \mid q_6 \mid q_5 \mid q_4 \mid q_3 \mid q_2 \mid |z|$$

which gives rise to

$$\ldots < q_7 < q_6 < q_5 < q_4 < q_3 < q_2 < |z|$$

But we know that such a sequence is necessarily finite.

§6. THE EUCLIDEAN RING Z, +, ., ⩽

We know that every $n \in \omega_0$ can be written

$$n = \underbrace{1 + \ldots + 1}_{n \text{ terms}}$$

Hence $n < \underbrace{1 + \ldots + 1}_{n \text{ terms}} + 1$

Therefore, for every $d \in \omega_0$ we again have

$$n < \underbrace{d + \ldots + d}_{n+1 \text{ terms}}$$

More simply

$$n < (n+1)d$$

The set of natural integers m such that $n < (m+1)d$ is thus a non-empty set. Denote by q the smallest natural integer of this set.

It follows that

$$n < (q+1)d$$

And since q is the smallest natural integer satisfying this condition it also follows that

$$qd \leqslant n < (q+1)d$$

If $qd = n$, we have $(-n) = (-q)d$.
If $qd \neq n$, we must have

$$qd < n < (q+1)d$$

Hence

$$(-(q+1))d < -n < (-(q+1)+1)d$$

We can therefore claim that

$$\forall z \in \mathrm{Z}, \forall d \in \omega_0, \exists q \in \mathrm{Z}: \quad qd \leqslant z < (q+1)d$$

Putting $r = z - qd$, we get

$$z = qd + r \quad \text{and} \quad 0 \leqslant r < d$$

We can therefore also affirm that

$$\forall z \in \mathrm{Z}, \forall d \in \omega_0, \exists q \in \mathrm{Z}, \exists r \in \mathrm{Z}: \quad z = qd + r \quad \text{and} \quad 0 \leqslant r < d$$

We can lift the restriction imposed on d by noting that

$$z = qd + r \quad \text{and} \quad 0 \leqslant r < d$$

is equivalent to

$$z = (-q)(-d) + r \quad \text{and} \quad 0 \leqslant r < |-d|$$

Euclid's Theorem

$$\forall z \in \mathrm{Z}, \forall d \in \mathrm{Z}_0, \exists q \in \mathrm{Z}, \exists r \in \mathrm{Z}: \quad z = qd + r \text{ and } 0 \leqslant r < |d|$$

§7. THE SUBMODULES OF Z, +

Submodules. For all (non-empty) subsets P of Z, we shall denote by mod P the submodule of Z, + generated by P.

By an abuse of notation, we shall write mod g instead of mod $\{g\}$ for all $g \in \mathrm{Z}$.

We then have

$$\mathrm{mod}\,\{g\} = \mathrm{mod}\,g = \mathrm{Z}g = \{zg \mid z \in \mathrm{Z}\}$$

We recall that a submodule S of Z is said to be cyclic if and only if there exists a $g \in \mathrm{Z}$ such that $\mathrm{S} = \mathrm{mod}\,g$.

Theorem – All the submodules of Z, + *are cyclic.*

Let M be a submodule of Z, +. If $\mathrm{M} = \{0\}$, it is perfectly obvious that M is cyclic ($\{0\} = \mathrm{mod}\,0 = \mathrm{Z} \cdot 0$).

If $\mathrm{M} \neq \{0\}$, there exists a z such that

$$0 \neq z \in \mathrm{M}$$

We have at once $-z \in \mathrm{M}$. And since one of the elements z, $-z$ belongs to ω_0 we can be sure that

$$\mathrm{M} \cap \omega_0 \neq \varnothing$$

Denote the smallest element of $\mathrm{M} \cap \omega_0$ by g.

We shall prove that

$$\mathrm{M} = \mathrm{Z}g = \mathrm{mod}\,g$$

Since $g \in \mathrm{M}$, we must have $\mathrm{Z}g \subset \mathrm{M}$.

It remains to show that $\mathrm{M} \subset \mathrm{Z}g$. (1)

For every $m \in \mathrm{M}$, there exists a $q \in \mathrm{Z}$ such that

$$qg \leqslant m < (q+1)g \tag{2}$$

Since $m \in \mathrm{M}$ and $qg \in \mathrm{M}$, we also have $m - qg \in \mathrm{M}$.

By the properties of ordered groups, formula (2) implies

$$0 \leqslant m - qg < g \tag{3}$$

Since g is the smallest strictly positive element of M, we cannot have $m - qg \neq 0$.

Thus $m = qg$ and we have established that every element m of M belongs to $\mathrm{Z}g$.

Q.E.D.

Corollary

For every non-empty subset P of Z, there exists one and only one element $g \in \omega$ such that $\mathrm{mod}\,\mathrm{P} = \mathrm{mod}\,g$. This element, which is denoted by $\wedge\,\mathrm{P}$, is a linear combination with rational integral coefficients of elements of P.

In other words: there exist elements $p_1, \ldots, p_n$ of P and rational integers $z_1, \ldots, z_n$ such that $\wedge\,\mathrm{P} = z_1 p_1 + \ldots + z_n p_n$.

Since the submodule mod P is cyclic, there exists a $z \in \mathrm{Z}$ such that $\mathrm{mod}\,\mathrm{P} = \mathrm{mod}\,z$. And since $\mathrm{mod}\,z = \mathrm{mod}\,|z|$, there therefore exists a $g \in \omega$ such that $\mathrm{mod}\,\mathrm{P} = \mathrm{mod}\,g$.

We know that $\mathrm{mod}\,x = \mathrm{mod}\,y \Rightarrow |x| = |y|$. (The reader should verify this.)

Thus there exists one and only one $g \in \omega$ such that $\mathrm{mod}\,\mathrm{P} = \mathrm{mod}\,g$.

We have $g \in \mathrm{mod}\,g$ and consequently $g \in \mathrm{mod}\,\mathrm{P}$. And we know that every element of mod P is a linear combination with rational integral coefficients of elements of P.

Special notation

For all elements $a, b \in \mathrm{Z}$ we shall put

$$a \wedge b = \wedge\{a, b\}$$

Exercises

1. $\forall z \in \mathrm{Z}: \quad \wedge\{z\} = |z|$
2. $\forall a, b \in \mathrm{Z}: \quad a \wedge b = b \wedge a$
   $a \wedge a = |a|$
3. $\forall a, b, c \in \mathrm{Z}: \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c = \wedge\{a, b, c\}$

§8. THE STRUCTURES Z, ∧, ∨ and ω, ∧, ∨

We introduced above the commutative inner law ∧ in Z. This law is entirely defined by

$$\forall a, b \in \mathrm{Z}: \quad \mathrm{mod}\,(a \wedge b) = \mathrm{mod}\,a + \mathrm{mod}\,b; \quad a \wedge b \in \omega$$

(see Ch. 5, §4)

We define similarly

$$\forall a, b \in \mathrm{Z}: \quad \mathrm{mod}\,(a \vee b) = \mathrm{mod}\,a \cap \mathrm{mod}\,b; \quad a \vee b \in \omega$$

Note that ω is stable for both the laws $\wedge$, $\vee$. Thus $\omega, \wedge, \vee$ is a substructure of Z, $\wedge$, $\vee$.

Both the laws $\wedge$, $\vee$ are commutative and associative.

We have already established these properties for the law $\wedge$. The commutativity and associativity of $\vee$ result from the commutativity and associativity of the intersection of submodules.

Exercise

Give a detailed proof of this statement.

Least common multiple

We are going to look for a new characterization of $a \vee b$.

The element $a \vee b$ is defined by

$$\text{mod}\,(a \vee b) = \text{mod}\,a \cap \text{mod}\,b, \qquad a \vee b \in \omega$$

But mod a is the set of multiples of a,
mod b is the set of multiples of b,
mod $(a \vee b)$ is the set of multiples of $a \vee b$.

Since mod $a \cap$ mod b is the set of multiples common to a and b, we see that

$a \vee b$ is the natural number whose set of multiples is precisely the set of multiples common to a and b.

We call $a \vee b$ the least common multiple of a and b.

Greatest common divisor (or Highest common factor)

We shall give a new definition of $\wedge$ P for every subset P of Z.

Let us recall that $\wedge$ P is defined by

$$\text{mod} \wedge \text{P} = \text{mod P}; \qquad \wedge \text{P} \in \omega \tag{1}$$

div P is the set of divisors common to all the elements of P. Thus if A and B are non-empty subsets of Z, we have

$$\text{A} \subset \text{B} \Rightarrow \text{div A} \supset \text{div B} \tag{2}$$

which implies that

$$\text{div}\,g \supset \text{div mod}\,g \tag{3}$$

More precisely, we shall establish that we have, in fact

$$\forall g \in \text{Z}: \qquad \text{div}\,g = \text{div mod}\,g \tag{4}$$

Taking (3) into account, in order to establish (4) it remains to prove that

$$\text{div}\,g \subset \text{div mod}\,g \tag{5}$$

which is obvious, since every divisor of g divides its multiples, i.e. the elements of mod g.

We shall prove the more general formula

$$\forall \text{P} \subset \text{Z}: \qquad \text{div P} = \text{div mod P} \tag{6}$$

Since P $\subset$ mod P, we have, by (2), div mod P $\subset$ div P (7)

On the other hand, mod P is the set of linear combinations with coefficients in Z of elements of P. Now, every divisor common to all the elements of P immediately divides every combination (with coefficients in Z) of such elements. (See the exercise below.)

Thus, every divisor common to all the elements of P is a divisor common to all the elements of mod P.

Hence div P $\subset$ div mod P (8)

Formula (6) follows from (7) and (8).

Taking into account formulae (1), (4) and (6) we have finally

$$\forall \text{P} \subset \text{Z}: \text{div} \wedge \text{P} = \text{div mod} \wedge \text{P} = \text{div mod P} = \text{div P}; \wedge \text{P} \in \omega \tag{9}$$

Thus $\wedge$ P is the positive rational integer whose set of divisors is precisely the set of divisors common to the elements of P.

We re-express this characteristic property by saying that

$\wedge$ P is the greatest common divisor (or highest common factor) of P.

Exercise

Let $d, x_1, \ldots, x_n, c_1, \ldots, c_n \in \text{Z}$.

$$d|x_1, \ldots d|x_n \Rightarrow d|c_1x_1 + \ldots + c_nx_n$$

§9. THE FACTORIAL RING Z, +, .

Proposition. If a and p denote rational integers: p prime and $p \nmid a \in \text{Z} \Rightarrow p \wedge a = 1$.

In other words:

If p is a prime natural integer which does not divide the rational integer a, we have $p \wedge a = 1$.

In fact, div $p = \{1, -1, p, -p\}$ and

$$p \notin \text{div}\,a, \qquad -p \notin \text{div}\,a$$

Consequently

$$\operatorname{div}\{a, p\} = \operatorname{div} p \cap \operatorname{div} a = \{1, -1\}$$

hence

$$a \wedge p = \wedge\{a, p\} = 1$$

Proposition. *If a, b, c denote rational integers:*

$$a|bc \quad \textit{and} \quad a \wedge b = 1 \Rightarrow a|c$$

There exist rational integers $a', b' \in \mathrm{Z}$ such that $a \wedge b = a'a + b'b$.
Therefore

$$1 = a'a + b'b \tag{1}$$

and

$$c = a'ac + b'bc \tag{2}$$

and hence $a|a'ac$ and $a|bc|b'bc$ imply $a|c$.

Q.E.D.

Theorem – If a, b, c denote rational integers, $a \wedge c = 1 \Rightarrow a \wedge b = a \wedge bc$.

We have $\operatorname{div}(a \wedge b) \subset \operatorname{div}(a \wedge bc)$ (since $\operatorname{div}(a \wedge b) = \operatorname{div}\{a, b\} \subset \operatorname{div}\{a, bc\} = \operatorname{div}(a \wedge bc)$), whence

$$a \wedge b \mid a \wedge bc \tag{3}$$

It remains to prove that

$$a \wedge bc \mid a \wedge b$$

Since $a \wedge c = 1$, there exist $a', c' \in \mathrm{Z}$ such that

$$1 = a'a + c'c \tag{4}$$

On the other hand $a \wedge b$ is a linear combination with rational integral coefficients of a and b.

$$a \wedge b = a''a + b''b \quad (\text{with } a'', b'' \in \mathrm{Z}) \tag{5}$$

Multiplying equations (4) and (5) term by term, we get

$$\begin{aligned} a \wedge b &= (a'a + c'c)(a''a + b''b) \\ &= (aa'a'' + a'bb'' + a''cc')a + (b''c')(bc) \end{aligned}$$

Therefore
$a \wedge b \in \operatorname{mod}\{a, bc\} = \operatorname{mod} \wedge\{a, bc\} = \operatorname{mod}(a \wedge bc) = (a \wedge bc)\mathrm{Z}$
Thus

$$a \wedge bc \mid a \wedge b$$

Q.E.D.

Corollary 1 – If a, b, c denote rational integers, $a \wedge b = 1$ and $a \wedge c = 1 \Rightarrow a \wedge (bc) = 1$.

Corollary 2 – If $a, b_1, b_2, \ldots b_n$ denote rational integers, $a \wedge b_1 = 1, \ldots, a \wedge b_n = 1 \Rightarrow a \wedge (b_1 b_2 \ldots b_n) = 1$.

Corollary 3 – If $p, p_1, \ldots, p_n$ denote prime integers, $|p| \neq |p_1|, \ldots, |p| \neq |p_n| \Rightarrow p \nmid p_1 \ldots p_n$.

Indeed

$$|p| \neq |p_i| \Leftrightarrow p \wedge p_i = 1$$

and

$$p \neq p_1, \ldots, p_n \Leftrightarrow p \wedge (p_1 \ldots p_n) = 1$$

Corollary 4 – If $p_1, \ldots, p_n$ and $p'_1, \ldots, p'_n$ denote primes

$$p_1 \ldots p_n = p'_1 \ldots p'_n \Rightarrow \begin{cases} n = n' \\ \text{There exists a permutation } f: \\ \qquad \{1, \ldots, n\} \to \{1, \ldots, n\} \\ \text{such that } |p_i| = |p'_{f(i)}| \end{cases}$$

Since $p_1 \mid p'_1 \ldots p'_n$, there exists $f_{(1)}$ such that

$$|p_1| = |p'_{f(1)}|$$

So p_2 must divide the product of the remaining p'.
Hence $|p_2| = |p'_{f(2)}|$.
Finally, $|p_{n-1}| = |p'_{f(n-1)}|$ and $|p_n| = |p'_{f(n)}|$.
Hence $n \leqslant n'$. By an analogous reasoning, $n' \leqslant n$.
By its construction, f was injective. It is therefore a permutation of $\{1, \ldots, n\}$.

Theorem – Every rational integer z admits a prime factorization and this is unique (in the sense of corollary 4 above).

This theorem is an immediate consequence of proposition 3 of §5 and of corollary 4 above.

We restate this last result by saying that the ring $\mathrm{Z}, +, .$ is factorial.

§10. FACTORIZATION IN ω

Prime factorizations

For every rational integer which is neither zero nor invertible, the natural integer $|z|$ admits a prime factorization.

$$|z| = p_1 \ldots p_n$$

where the p_i are strictly positive primes.

If $z = -|z|$, we get $z = (-1) \cdot p_1 \cdots p_n = (-p_1) \cdot p_2 \cdots p_n$.

Thus the prime factorizations of the rational integers are obtainable in a very simple way from the prime factorizations of the natural integers in ω. Therefore the indications are that we should deal systematically with ω for the study of factorizations. We shall do this up to the end of this paragraph.

This convention having been implicitly accepted, the enunciation of the prime factorization theorem is simplified.

Theorem – Every natural number (not 0 or 1) admits a unique prime factorization (up to the order of the factors).

Examples

$$12 = 2.2.3$$
$$4 = 2.2$$
$$8 = 2.2.2$$
$$625 = 5.5.5.5$$
$$7 = 7$$
$$84 = 2.2.3.7$$

Exercise

Denote the set of primes of ω by Π. For every $n \in \omega$, we represent the set of prime divisors of n by $p(n)$. Then we have

$$p(n) = \{x \in \Pi \mid x|n\}$$
$$p(0) = \Pi$$
$$p(1) = \varnothing$$

By introducing the notation $p(n)$, we have, in fact, defined a map

$$p : \omega \to \mathscr{P}\Pi : n \to p(n)$$

The function p maps ω_0 *onto* the set of finite subsets of Π. Two distinct natural numbers $x \neq y$ may have the same image by p

$$p(6) = p(12) = p(48) = p(18) = \{2, 3\}$$

If a, b denote natural numbers

$$a|b \Rightarrow p(a) \subset p(b)$$
$$p(1) \subset p(a) \subset p(0)$$

For every natural number $n \neq 0$, denote by $sp(n)$ the product of the primes of $p(n)$.

Then we have $sp(48) = sp(12) = sp(6) = 6$

$$sp(a)|sp(b) \Leftrightarrow p(a) \subset p(b)$$

Theorem – There does not exist a greatest prime number.

It is sufficient to prove that for every $n \in \omega$, there exists a prime greater than n.

We know that there exists a prime p which divides the natural number $n! + 1$. And $n! + 1$ is not divisible by any prime $\leqslant n$.

Therefore $p > n$.

Q.E.D.

Primary factorizations

Every positive integral power of a prime is called a *primary* (number).

If p is prime, for every $n \in \omega_0$ the natural number p^n is primary and n is the exponent of the primary p^n and p its prime.

Examples

625 is a primary of prime 5 and exponent 4.
2, 4, 8, 1024, 3, 9, 7, 49, 121 are primaries.
0, 1, 6, 18, 24 are not primaries.

Exercises

1. The prime numbers are primaries of exponent 1.

2. Every divisor of a primary (except the trivial divisors ± 1) is a primary with the same prime and exponent less than or equal to that of the primary.

3. Every positive integral power of a primary is a primary.

4. With the notations of the exercise of §10, x primary $\Leftrightarrow sp x$ prime.

5. Show that x primary $\Leftrightarrow \# p(x) = 1$.

If we associate the equal prime factors in a prime factorization, we get a primary factorization.

$$n = p_1^{e_1} \ldots p_s^{e_s}$$

We always assume implicitly that the p_i are distinct primes one from the other and the e_i non-zero natural numbers.

Examples of primary factorizations

$$240 = 2^4.3.5$$
$$625 = 5^4.$$
$$2 = 2$$

The theorem on the prime factorization of the natural numbers enables us to enunciate

Theorem – Every natural number (differing from 0 *and* 1*) admits a unique primary factorization (up to the order of the factors).*

Corollary – If q is a primary dividing the product of primaries $p_1^{e_1} \dots p_s^{e_s}$, there exists an i such that $q = p_i^{s_i}$ with $1 \leqslant s_i \leqslant e_i$.

Exercise—Prove the above corollary.

§11. SETS OF DIVISORS AND FILTERING SETS

Here we denote by $\operatorname{div} n$, $n \in \omega$ the set of natural divisors of n, i.e. the set of divisors of n which are natural numbers.

Obviously:

$$x|y \in \operatorname{div} n \Rightarrow x \in \operatorname{div} n$$

We restate this proposition by saying that the set of natural divisors of a natural number is a *filtering* (set) of the ordered set $\omega, |$.

In general, we say that the subset P of the ordered set E, $\prec$ is a filtering (set) if and only if

$$x \prec y \in \mathrm{P} \Rightarrow x \in \mathrm{P}$$

Examples and Exercises

1. The set $\mathscr{P}\mathrm{A}$ of subsets of $\mathrm{A} \subset \mathrm{E}$ is a filtering subset of $\mathscr{P}\mathrm{E}, \subset$.

2. For every subset P of ω, the set $\operatorname{div}\mathrm{P}$ is a filtering subset of $\omega, |$.

3. $\{1, 3, 5, 15, 25, 75\}$ is a filtering subset of $\omega, |$.

4. $\{1, 2, 8\}$ is not a filtering subset of $\omega, |$.

5. If F is a non-empty filtering subset of $\omega, |$, we have $1 \in \mathrm{F}$.

6. If the filtering subset F of $\omega, |$ contains 0, we have $\mathrm{F} = \omega$.

7. If $\mathscr{F}$ is a non-empty filtering subset of $\mathscr{P}\mathrm{E}, \subset$, we have $\varnothing \in \mathscr{F}$. If E belongs to the filtering subset $\mathscr{F}$ of $\mathscr{P}\mathrm{E}, \subset$, we have $\mathscr{F} = \mathscr{P}\mathrm{E}$.

8. Let $\mathrm{A} \subset \mathrm{E}$. The set $\mathscr{A}$ of subsets of E which contain A is a filtering subset of $\mathscr{P}\mathrm{E}, \supset$.

9. The filtering subsets of $\mathrm{R}, \leqslant$ are
   (1) the empty set
   (2) the set R itself
   (3) the open half-lines $\{x \in \mathrm{R} \mid x < r\}$
   (4) the closed half-lines $\{x \in \mathrm{R} \mid x \leqslant r\}$.

10. A subset P of $\omega, |$ is a filtering if and only if

$$x \in \mathrm{P} \Rightarrow \operatorname{div} x \subset \mathrm{P}$$

11. A subset $\mathscr{F}$ of $\mathscr{P}\mathrm{E}, \subset$ is a filtering $\Leftrightarrow (\mathrm{X} \in \mathscr{F} \Rightarrow \mathscr{P}\mathrm{X} \subset \mathscr{F})$.

We leave to the reader the pleasure of proving the

Theorem – Every intersection and every union of filtering sets of an ordered set is a filtering set.

Denote by $\mathscr{H}$ the set of primaries.

Since $\mathscr{H}$ is a subset of ω, the set $\mathscr{H}$ has an ordering $|$.

Proposition. For every $n \in \omega$, the set $q(n)$ of primary divisors of n is a filtering subset of $\mathscr{H}, |$.

If $n \neq 0$, the filtering set $q(n)$ is finite, whereas $q(0) = \mathscr{H}$ is infinite. Conversely, every finite filtering subset of $\mathscr{H}, |$ is the set $q(n)$ of primary divisors of some natural number n.

We shall leave to the reader the task of establishing that $q(n)$ is a filtering subset of $\mathscr{H}, |$. We note in passing that $q(n)$ is a filtering subset of $\omega, |$ only for $n = 1$. (In this case $q(n) = \varnothing$.)

Instead of saying that $q(n)$ is a filtering subset of $\mathscr{H}, |$ we shall say that $q(n)$ *is a filtering set of primaries.*

Let us show that every finite filtering set of primaries is the set $q(n)$ of primary divisors of a particular natural number $n \in \omega_0$.

Let F be a finite filtering subset of $\mathscr{H}, |$.

If $\mathrm{F} = \varnothing$, we have $\mathrm{F} = q(1)$. We assume therefore that $\mathrm{F} \neq \varnothing$.

Every $x \in \mathrm{F}$ is a primary and is written $x = p^e$ where p is prime and $e \in \omega_0$. The set of primaries of F having p as prime is therefore a finite non-empty set. Consequently, one of these primaries has a maximum exponent. We shall say that such a primary is maximal (because it does not divide strictly any other element of F).

We have therefore just shown that every element of F divides a maximal primary of F.

Since F is finite, so, *a fortiori*, is the set of its maximal primaries.

Let us denote them by $p_1^{m_1}, \ldots, p_s^{m_s}$ and let us put $n = p_1^{m_1} \ldots p_s^{m_s}$.

We shall prove that $\mathrm{F} = q(n)$.

Let $x \in \mathrm{F}$. The number x is primary and we have just seen that it divides one of the maximal primaries of F. It is therefore a primary divisor of n. Hence $x \in q(n)$. We have just established that $\mathrm{F} \subset q(n)$.

Conversely, every primary divisor of n is of the form $p_i^{e_i}$ with

$$p_i^{e_i} \mid p_i^{m_i} \in \mathrm{F}$$

Since F is filtering, we therefore have $p_i^{e_i} \in \mathrm{F}$. Thus $q(n) \subset \mathrm{F}$.

Q.E.D.

An isomorphism of ordered sets

Consider on the one hand the ordered set $\omega, |$.

Now put $\Phi = \{q(n) \} n \in \omega\}$.

The elements of Φ are therefore

the finite filtering sets of primaries

the set $\mathscr{H}$ of primaries of ω.

Having made this definition, let us consider the ordered set $\Phi, \subset$.

In defining $q(n)$ we have in fact defined a map $q : \omega \to \Phi : n \to q(n)$.

As a result of the uniqueness of prime factorization, we have

$$\forall a, b \in \omega: \qquad a = b \Leftrightarrow q(a) = q(b)$$

Thus q is a bijection of ω onto Φ.

Proposition. $\forall a, b \in \omega: \qquad a|b \Leftrightarrow q(a) \subset q(b)$ (1)

If $a|b$ every primary divisor of a is a primary divisor of b and $q(a) \subset q(b)$.

Let $b = p_1^{e_1} \ldots p_s^{e_s}$.

Since $q(a) \subset q(b)$, every primary divisor of a is a primary divisor of b. Therefore every primary divisor of a is of the form $p_i^{k_i}$ with $1 \leqslant k_i \leqslant e_i$ (for some value of i).

Since a is the product of its maximal primary divisors we then have $a = p_1^{k_1} \ldots p_s^{k_s}$ with $0 \leqslant k_i \leqslant e_i$.

Thus $a|b$.

Definition. We express the fact that q is a bijection $\omega \to \Phi$ satisfying (1) *by saying that q is an isomorphism of the ordered set $\omega, |$ onto the ordered set $\Phi, \subset$.*

§12. THE DISTRIBUTIVE LATTICE $\omega, \wedge, \vee$

We know that q is an isomorphism of ordered sets

$$q : \omega, | \to \Phi, \subset$$

We have defined the laws $\wedge$ and $\vee$ in $\omega, |$.

The laws $\wedge$ and $\vee$ are completely defined by the structure of the ordering $\omega, |$, and the laws $\cap$ and $\cup$ are defined in the same way in $\Phi, \subset$.

Since the union and intersection of filtering sets are filtering sets and every finite filtering set of primaries is the set of primary divisors of a natural number, the set Φ is stable for $\cap$ and $\cup$. Thus we can speak of the structure $\Phi, \cap, \cup$.

In fact, $\wedge, \vee$ are the infimum and the supremum for the ordered set $\omega, |$ while $\cap$ and $\cup$ are the infimum and the supremum in the ordered set $\Phi, \subset$.

It follows that

$$q(a \wedge b) = q(a) \cap q(b)$$
$$q(a \vee b) = q(a) \cup q(b)$$

By the isomorphism

$$q : \omega, \wedge, \vee \to \Phi, \cap, \cup$$

the properties of the structure $\omega, \wedge, \vee$ are carried over to $\Phi, \cap, \cup$ and conversely.

Thus, the mutual distributivity of $\cap$ and $\cup$ implies the mutual distributivity of $\wedge$ and $\vee$.

Theorem – The laws $\wedge$ and $\vee$ *defined on* ω *are mutually distributive. In other words*:

$$\forall a, b, c \in \omega: \qquad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$
$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

More simply:

The lattice $\omega, |, \wedge, \vee$ *is distributive.*

§13. UTILIZATION OF THE PROPERTIES OF Z, + IN THE STUDY OF GROUPS

Let G, $*$ be any group whatsoever and g one of its elements. We say that g is of finite order n if and only if n is the smallest natural integer such that $n \perp g = \nu$. In this case, the cyclic group generated by g is itself of order n.

Indeed we know that

$$\text{grp}\,(g) = \mathrm{Z} \perp g = \{z \perp g \,|\, z \in \mathrm{Z}\}$$

But every $z \in \mathrm{Z}$ may be written

$$z = qn + r \quad \text{with} \quad q \in \mathrm{Z},\ 0 \leqslant r < n$$

Therefore

$$\begin{aligned} z \perp g &= (qn + r) \perp g \\ &= ((qn) \perp g) * (r \perp g) && \text{by (Ch. 3, §4.1)} \\ &= (q \perp (n \perp g)) * (r \perp g) && \text{by (Ch. 3, §9.1)} \\ &= (q \perp \nu) * (r \perp g) && \text{because } n \perp g = \nu \\ &= \nu * (r \perp g) && \text{by (Ch. 3, §11 Ex. 3,)} \\ &= r \perp g && \text{by the definition of the neuter of a group} \end{aligned}$$

Consequently

$$\text{grp}\,(g) = \mathrm{Z} \perp g = \{r \perp g \,|\, r \in \{0, 1, 2, \ldots, n-1\}\}$$

It remains to prove that if a and b are two natural numbers strictly smaller than n, we have

$$a \neq b \Rightarrow a \perp g \neq b \perp g$$

We may assume that $a < b$. The equality $a \perp g = b \perp g$ would imply $(b - a) \perp g = \nu$ which is impossible since $0 < b - a < n$. The proposition is thus established.

If g is not of finite order, we must have $\text{grp}\, g = \mathrm{Z} \perp g$ where

$$\forall x, y \in \mathrm{Z}: \qquad x \neq y \Rightarrow x \perp g \neq y \perp g$$

(Indeed if this were not so, we could assume $x < y$ with $x \perp g = y \perp g$ and hence $(y - x) \perp g = \nu$ where $y - x$ is a non-zero natural number, which would imply that g is of finite order.)

Theorem 1 – *In a group of finite order, all the elements are themselves of finite order and the order of every element divides the order of the group.*

(We have in fact seen that if an element is not of finite order, it generates an infinite group, which is impossible in a group of finite order. On the other hand, the order of an element is *ipso facto* the order of a subgroup and therefore a divisor of the order of the group.)†

† Tr.. See Ch 4, §13.

Proposition 1. *If g is an element of order n, we have* $\forall z \in \mathrm{Z}$: $z \perp g = \nu \Leftrightarrow n|z$.

If $n|z$, put $z = qn$. Hence $z \perp g = (qn) \perp g = q \perp (n \perp g) = q \perp \nu = \nu$, which establishes the implication $\Leftarrow$.

Conversely, let $z \perp g = \nu$. Put $z = nq + r$. $z \perp g = \nu$ then implies $r \perp g = \nu$ and therefore $r < n$ means that $r = 0$, which establishes the implication $\Rightarrow$.

Proposition 2. *If g is an element of finite order n of a group* G, $*$, *we have* $\forall x, y \in \mathrm{Z}$: $x \perp g = y \perp g \Leftrightarrow n|(x - y)$, *or its equivalent* $\forall x, y \in \mathrm{Z}$: $x \perp g = y \perp g \Leftrightarrow \dfrac{x}{n} = \dfrac{y}{n}$ (where we use the notations of Chapter 2, e).

Exercise

Prove this proposition.

Proposition 3. *If g is an element of finite order of a group* G, $*$ *and if $d|n$, the element $d \perp g$ is of order n/d.*

Put $n = qd$ (therefore $q = n/d$).

We have

$$n \perp g = (qd) \perp g = q \perp (d \perp g)$$

Consequently, since n is the smallest integer such that $n \perp g = \nu$, the quotient n/d is the smallest integer such that

$$q \perp (d \perp g) = \nu$$

Q.E.D.

Proposition 4. *Let g be an element of finite order n of the group* G, $*$ *and let k be a natural number such that $k \wedge n = 1$. The element $k \perp g$ is then of finite order n.*

Moreover, $\text{grp}\,(k \perp g) = \text{grp}\, g$.

Since $k \perp g \in \text{grp}\, g$, we have $\text{grp}\,(k \perp g) \subset \text{grp}\, g$.

It remains to prove that $\text{grp}\, g \subset \text{grp}\,(k \perp g)$.

To do this, it is sufficient to establish that $g \in \text{grp}\,(k \perp g)$, i.e. that there exists $z \in \mathrm{Z}$ such that $g = z \perp (k \perp g)$.

Now $k \wedge n = 1$ implies the existence of rational integers k' and n' such that

$$1 = k'k + n'n$$

Hence

$$\begin{aligned} g = 1 \perp g &= (k'k + n'n) \perp g \\ &= (k'k) \perp g * (n'n) \perp g \\ &= k' \perp (k \perp g) * n' \perp (n \perp g) \\ &= k' \perp (k \perp g) * n' \perp \nu \\ &= k' \perp (k \perp g) * \nu \\ &= k' \perp (k \perp g) \end{aligned}$$

Q.E.D.

Revision exercises on Chapter 6

1. Let $d, x_1, x_2, \ldots, x_n \in \mathrm{Z}$. We have: $(d|x_1, d|x_2, \ldots, d|x_n) \Rightarrow d|(x_1 + x_2 + \ldots + x_n)$. In fact, since $d|x_1$, we have $x_1 \in \mathrm{mod}\, d$. Then $x_1, \ldots, x_n \in \mathrm{mod}\, d$ and $x_1 + \ldots + x_n \in \mathrm{mod}\, d$, hence $d|x_1 + \ldots + x_n$.

2. Let $d, x, c \in \mathrm{Z}$. We have $d|x_1 \Rightarrow d|cx_1$.

3. Let $z, d, z' \in \mathrm{Z}$. Prove that the remainder after the division of z by d is equal to the remainder of the division of $z + z'd$ by d.

4. Let $z, d \in \mathrm{Z}$. We know that

$$\exists q \in \mathrm{Z}, \exists r \in \mathrm{Z}: \quad z = dq + r, \quad 0 \leqslant r < |d|$$

Prove

(a) $d_1|z$ and $d_1|d \Rightarrow d_1|r$
(b) $d_1|d$ and $d_1|r \Rightarrow d_1|z$.

5. (1) $\forall a, b \in \mathrm{Z}: \quad (a|a \wedge b) \wedge (b|a \wedge b) = 1$.
(2) $(d \in (\omega \cap \mathrm{div}\, \{a, b\})$ and $(a|d) \wedge (b|d) = 1) \Rightarrow d = a \wedge b$.
(3) Condense 1 and 2 into a single proposition.

6. The G.C.D. (or H.C.F.) of a set P of integers is not altered if we replace two elements of P by their G.C.D.
In fact:

$$\begin{aligned} \mathrm{mod}\, (\wedge \{x_1, x_2, \ldots, x_n\}) &= \mathrm{mod}\, \{x_1, x_2, \ldots, x_n\} \\ &= \mathrm{mod}\, x_1 + \mathrm{mod}\, x_2 + \ldots + \mathrm{mod}\, x_n \\ &= \mathrm{mod}\, \{x_1, x_2\} + \mathrm{mod}\, x_3 + \ldots + \mathrm{mod}\, x_n \\ &= \mathrm{mod}\, (\wedge \{x_1, x_2\}) + \mathrm{mod}\, x_3 + \ldots \\ &\qquad + \mathrm{mod}\, x_n \\ &= \mathrm{mod}\, (\wedge \{\wedge \{x_1, x_2\}, x_3, \ldots, x_n\}). \end{aligned}$$

7. Let $x_1, x_2, \ldots, x_n, d \in \mathrm{Z}$.
(a) $(d|x_1, d|x_2, \ldots, d|x_n) \Rightarrow d| \wedge \{x_1, x_2, \ldots, x_n\}$.
For: by hypothesis $x_1, x_2, \ldots, x_n \in \mathrm{mod}\, d$. It follows that $\mathrm{mod}\, \{x_1, x_2, \ldots, x_n\} \subset \mathrm{mod}\, d$. Now: $\mathrm{mod}\, \{x_1, x_2, \ldots, x_n\} = \mathrm{mod}\, (\wedge \{x_1, x_2, \ldots, x_n\})$, which implies $\wedge \{x_1, x_2, \ldots, x_n\} \in \mathrm{mod}\, d$.

Q.E.D.

(b) $d| \wedge \{x_1, x_2, \ldots, x_n\} \Rightarrow (d|x_1, d|x_2, \ldots, d|x_n)$.
(c) Enunciate (a) and (b) as a single proposition.

8. If $x_1, x_2, \ldots, x_n \in \mathrm{Z}$ and $c \in \omega$, we have $\wedge \{cx_1, cx_2, \ldots, cx_n\} = c \,.\, \wedge \{x_1, x_2, \ldots, x_n\}$.

9. Let $x_1, x_2, \ldots, x_n \in \mathrm{Z}$ and $d \in \omega \cap \mathrm{div}\, \{x_1, \ldots, x_n\}$.
We then have $\wedge \{x_1/d, x_2/d, \ldots, x_n/d\} = \wedge \{x_1, \ldots, x_n\}/d$.

10. $\forall x_1, \ldots, x_n \in \mathrm{Z}, d \in \omega \cap \mathrm{div}\, \{x_1, \ldots, x_n\}$:
(a) $\wedge \{x_1/ \wedge \{x_1, \ldots, x_n\}, \ldots, x_n/ \wedge \{x_1, \ldots, x_n\}\} = 1$.
(b) $\wedge \{x_1/d, \ldots, x_n/d\} = 1 \Rightarrow d = \wedge \{x_1, \ldots, x_n\}$.
(c) Enunciate (a) and (b) as a single proposition.

11. In every ring A, +, . we have for every $a, b, c \in \mathrm{A}$:
(1) $-(-a) = a$;
(2) $a(b - c) = ab - ac$,
$(a - b)c = ac - bc$;
(3) $a0 = 0a = 0$;
(4) $(-a)b = -(ab)$,
$a(-b) = -(ab)$;
(5) $(-a)(-b) = ab$.

12. Prove that $\{a + bi \mid a, b \in \mathrm{Z}\}$, +, ., where the laws are the laws induced by those of C, is a ring (which we call the ring of GAUSSIAN integers).

13. Let G, + be a commutative group. We obtain a ring G, +, . by putting $\forall a, b \in \mathrm{G}: a.b = 0$.

14. Let $\mathrm{Z}_2 = \{0, 1\}$. We have already considered the cyclic group Z_2, + defined by

+	0	1
0	0	1
1	1	0

Prove that by providing Z_2 with a second law . by putting

·	0	1
0	0	0
1	0	1

$Z_2, +, .$ is a ring.

15. The structure $Z_3, +, .$ defined by

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

is a ring.

16. The ring of polynomials: A[X], $+, .$.

Consider a ring A, $+, .$. Every expression of the form

$$a_0X^0 + a_1X^1 + \ldots + a_nX^n$$

where $a_0, a_1, \ldots, a_n \in A$, and where X is a letter (which does not belong to A), is called a polynomial in X with coefficients in A.

We make the following definitions:

definition 1. $\sum a_iX^i = \sum b_iX^i \Leftrightarrow \forall i \in \omega : a_i = b_i$.

definition 2. $\sum_{i=0}^{n} a_iX^i + \sum_{i=0}^{n} b_iX^i = \sum_{i=0}^{n} (a_i + b_i)X^i$.

definition 3. $\sum_{i=0}^{m} a_iX^i . \sum_{j=0}^{n} b_jX^j = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_ib_j \right) X^k$.

The set of polynomials in X with coefficients in A, provided with the laws + and . thus defined is a ring. This ring is called the ring of polynomials in X with coefficients in A, and is denoted by A[X], $+, .$.

17. Determine the order of each element of the cyclic group $Z_{12}, +$ (see §13, propositions 3, 4).

18. Determine the order of each element of the cyclic group $Z_{11}, +$.

19. Determine the order of each element of the cyclic group $Z_p, +$ with p prime.

20. Let $\begin{pmatrix} 1 & 2 & 3 & 4 \ldots n-1 \\ 2 & 3 & 4 & 5 \ldots \quad 1 \end{pmatrix}$ be a permutation of $\{1, 2, 3, 4, \ldots, n-1, n\}$.

What is the order of this permutation?

21. What are the orders of the elements of Klein's four-group?

22. What are the orders of the elements of the group $\mathcal{S}_3, \circ$ (the symmetric group of degree 3)?

23. If $q(n)$ denotes the set of primary divisors of n, we have $q(1) = \varnothing$.

24. Let P be a set of primaries. Denote by ρP the set obtained by replacing every primary p^n of P by p^{n-m+1} where p^m denotes the smallest primary of prime p belonging to P. It follows that for every $a, b \in \omega_0$ such that $b|a$

$$q(a/b) = \rho(q(a) \setminus q(b))$$

7

Homomorphisms and Quotient Groups

§1. THE GROUP R, + AND PLANE ROTATIONS

We know that R, + constitutes a commutative group and that the real numbers may be represented by non-terminating decimals. On the other hand, we know that plane rotations with given centre are defined by their angles, and that depending on the choice of an orientation these may be represented in grades‡ by non-terminating decimals deprived of their integral part. The addition of angles is then expressed by the natural addition of these amputated decimals.

If in the decimal representation of a real number we suppress the integral part, we obtain an expression for an angle and therefore of a rotation (the centre of rotation and orientation having been fixed once and for all).

For every real number r, denote by $h(r)$ the rotation which r defines by the procedure we have just described.

If $r_1, r_2 \in \mathrm{R}$, we obviously have

$$h(r_1 + r_2) = h(r_1) \circ h(r_2) \tag{1}$$

In fact h is a map of the group R, + into the group R, $\circ$ of rotations with fixed centre. We indicate that this map satisfies formula (1) by saying that h is a homomorphism of the group R, + into the group $\mathscr{R}$, $\circ$.

§2. HOMOMORPHISM

A map $h : \mathrm{A} \to \mathrm{B}$ is called a homomorphism of the group A, $*$ into the group B, $\triangledown$ if it respects the group laws, i.e. if $h(x * y) = h(x) \triangledown h(y)$.

Every injective† homomorphism is called a monomorphism, and every projective† homomorphism is called an epimorphism.

Every bijection $f : \mathrm{A} \to \mathrm{B}$ such that f and f^{-1} are homomorphisms

† Tr. See Appendix.
‡ Tr. See Ch. 5, §1.

is called an isomorphism of the group A, $*$ onto the group B, $\triangledown$.

We often indicate that h is a homomorphism of A, $*$ into B, $\triangledown$ by writing

$$h : \mathrm{A}, * \to \mathrm{B}, \triangledown$$

Two groups A, $*$ and B, $\triangledown$ are said to be *isomorphic* if there exists an isomorphism $\mathrm{A}, * \to \mathrm{B}, \triangledown$.

When we studied the general properties of any group we were in the habit of using the sign $*$ for the law of the group. Thus we shall study the homomorphism of a group G, $*$ into a group H, $*$ using the same sign $*$ for the laws in G and H.

§3. EXAMPLES AND EXERCISES

1. Let A, $*$ and B, $*$ be groups. Every homomorphism $h : \mathrm{A}, * \to \mathrm{B}, *$ is an epimorphism $\mathrm{A}, * \to h\mathrm{A}, *$. Every monomorphism $m : \mathrm{A}, * \to \mathrm{B}, *$ is an isomorphism $\mathrm{A}, * \to m\mathrm{A}, *$.

The homomorphism $h : \mathrm{G}, * \to \mathrm{H}, *$ is an isomorphism if and only if h is a monomorphism and an epimorphism.

2. Let f be a bijection of the group A, $*$ onto the group B, $\triangledown$. If f is a homomorphism, then f^{-1} is a homomorphism.

3. We know that R, + ; $\mathrm{R}_0, .$ and $\mathrm{R}_0^+, .$ are groups. The exponential function

$$\exp : \mathrm{R} \to \mathrm{R}_0 : x \to \exp(x) = e^x$$

is a monomorphism $\mathrm{R}, + \to \mathrm{R}_0, .$. It is also an isomorphism $\mathrm{R}, + \to \mathrm{R}_0^+, .$.

The inverse map $\exp^{-1} = \log$ is an isomorphism $\mathrm{R}_0^+, . \to \mathrm{R}, +$.

4. The transformation t of Z

$$t : \mathrm{Z} \to \mathrm{Z} : x \to 2x$$

is a monomorphism $\mathrm{Z}, + \to \mathrm{Z}, +$.

It is also an isomorphism

$$t : \mathrm{Z}, + \to 2\mathrm{Z}, +$$

5. The map $\mathrm{R} \to \mathrm{R}/\mathrm{Z} : n \cdot d_1 d_2 \ldots \to \cdot d_1 d_2 \ldots$ is an epimorphism $\mathrm{R}, + \to \mathrm{R}/\mathrm{Z}, +$.

6. The multiplicative subgroup generated by -1 in the group $\mathrm{R}_0, .$;

the group of permutations of a pair;
the group $\mathscr{P}\{a\}, \Delta$;
the subgroup generated by a symmetry in the group of permutations of the plane;
the subgroup generated by $\cdot 5$ in $R/Z, +$
are all isomorphic groups.

7. The map $Z \to Z_2 : z \to \frac{z}{2}$ is an epimorphism $Z, + \to Z_2, +$.

8. Which are the homomorphisms amongst the following transformations of the group $R_0, .$?

(a) $x \to x$
(b) $x \to x^2$
(c) $x \to x^3$
(d) $x \to x^4$
(e) $x \to -x$
(f) $x \to -x^2$
(g) $x \to 2x$
(h) $x \to 3x$
(i) $x \to 1/x$
(j) $x \to -1/x$
(k) $x \to |x|$
(l) $x \to \sqrt{|x|} > 0$

9. The orthogonal projection of ordinary space E onto a plane Π defines an epimorphism of the group of translations of the space onto the group of translations of the plane.

Let Π, Π' be two planes of ordinary space E. Prove that the group of translations of Π is isomorphic to the group of translations of Π'.

10. The subgroup generated by i in $C_0, .$;
the subgroup generated by a rotation of an angle of $\cdot 25$ in $R/Z, +$;
the group $Z_4, +$;
are isomorphic groups.

11. Let $G, *$ be a group. We shall denote by G^n the set of sequences of n elements of G.

It is easy to show that $G^n, *$ is a group for the law $*$ defined by

$$(a_1, a_2, \ldots, a_n) * (b_1, b_2, \ldots, b_n) = (a_1 * b_1, a_2 * b_2, \ldots, a_n * b_n)$$

If the set E consists of n elements, the reader should establish the isomorphism

$$\mathscr{P}E, \Delta \to Z_2^n, +$$

12. If S is a subgroup of the group $G, *$, the identical map $S \to G : s \to s$ is a monomorphism $S, * \to G, *$.

13. Let h_1 and h_2 be homomorphisms of groups

$$h_1 : G_1, * \to G_2, *$$
$$h_2 : G_2, * \to G_3, *$$

The composite map $h_2 \circ h_1 : G_1 \to G_3$ is a homomorphism $G_1, * \to G_3, *$.

If h_1 and h_2 are monomorphisms, so is $h_2 \circ h_1$.
If h_1 and h_2 are epimorphisms, so is $h_2 \circ h_1$.
If h_1 and h_2 are isomorphisms, so is $h_2 \circ h_1$.
If $h_2 \circ h_1$ is a monomorphism, so is h_1.
If $h_2 \circ h_1$ is an epimorphism, so is h_2.

14. Let $\mathscr{G}$ be a set of groups. Isomorphism defines an equivalence in $\mathscr{G}$.

15. Let $A, *$ be a group and f a bifunction $A \to B$. Make B a group by providing it with a law $*$ defined by

$$\forall x, y \in A: \qquad f(x) * f(y) = f(x * y)$$

The bifunction f then becomes an isomorphism $A, * \to B, *$.

When we procede in this way, we say that we have carried over the structure of $A, *$ onto B.

16. The transformation t of R_0 defined by $t(x) = 1$ for $x > 0$ and $t(x) = -1$ for $x < 0$ is a homomorphism $R_0, . \to R_0, ..$ (We also say that it is an endomorphism of $R_0, ..$)

The image of t is $\{1, -1\}$ which is a subgroup of $R_0, ..$

17. Definitions: Every homomorphism $G, * \to G, *$ of a group $G, *$ is called an *endomorphism* of $G, *$.

Every isomorphism $G, * \to G, *$ is called an *automorphism* of $G, *$.

18. The map $f : Q_0^+ \to Z : 2^z(z_1/z_2) \to z$ (with $2 \nmid (z_1 z_2)$) is an epimorphism

$$f : Q_0^+, . \to Z, +$$

19. Following the notations of set theory, we denote by Z^{ω_0} the set of sequences $(z_1, z_2, \ldots, z_n, \ldots)$ of rational integers. The

natural definition of addition of sequences makes Z^{ω_0} into a group $Z^{\omega_0}, +$.† We shall denote by $Z^{(\omega_0)}$ the set of almost null sequences, i.e. consisting of only a finite number of non-null elements. It is easy to see that $Z^{(\omega_0)}, +$ is a subgroup of $Z^{\omega_0}, +$.

The map

$$Q_0^+ \to Z^{\omega_0} : 2^{z_1}.3^{z_2}.5^{z_3}.7^{z_4}.11^{z_5}.13^{z_6}\ldots \to (z_1, z_2, z_3, z_4, \ldots)$$

is a homomorphism $Q_0^+, . \to Z^{\omega_0}, +$.

It is an isomorphism $Q_0^+, . \to Z^{(\omega_0)}, +$.

20. Denote the set of natural primes (the number 1 excluded) by Π. The permutation p of Π defines the isomorphism

$$f : Q_0^+, . \to Q_0^+, . : 2^{z_1}3^{z_2}5^{z_3}\ldots \to p(2)^{z_1}.p(3)^{z_2}.p(5)^{z_3}\ldots$$

We also say that f is an automorphism of $Q_0^+, .$.

21. The map $x \to x^2$ defines an endomorphism of $R_0, .$, an epimorphism $R_0, . \to R_0^+, .$ and an automorphism of $R_0^+, .$.

The map $x \to x^3$ defines an automorphism $R_0, . \to R_0, .$.

22. Let $G, *$ be a group. The set of automorphisms of $G, *$ provided with the law $\circ$ is a group.

§4. THE IMAGE OF A HOMOMORPHISM

Proposition. Let $h : G, * \to H, *$ be a homomorphism of groups. The image $hG = \{h(x) \mid x \in G\}$ of the homomorphism h is a subgroup of $H, *$.

(a) Let us first establish that the image $h(\nu)$ of the neuter ν of $G, *$ is the neuter of $H, *$. It is sufficient to show that $h(\nu)$ is an idempotent of $H, *$. Since h is a homomorphism, we have $h(\nu * \nu) = (h(\nu) * (h(\nu))$. Hence

$$(h(\nu)) * (h(\nu)) = h(\nu * \nu) = h(\nu)$$

which establishes the idempotence of $h(\nu)$.

(b) We next prove that the image $h(\bar{x})$ of the symmetric of $x \in G$ is the symmetric $\overline{h(x)}$ of the image $h(x)$ of x.

Since h is a homomorphism, we have $h(x * \bar{x}) = h(x) * h(\bar{x})$, hence $h(x) * h(\bar{x}) = h(x * \bar{x}) = h(\nu) = \nu$, and finally

$$h(\bar{x}) = \overline{h(x)}$$

† Tr. Addition is defined by $(x_1, x_2, \ldots x_n, \ldots) + (y_1, y_2, \ldots y_n, \ldots) = (x_1 + y_1, x_2 + y_2, \ldots x_n + y_n, \ldots)$

(c) The homomorphism h respects not only the law $*$,

$$\forall x, y \in G: \quad h(x * y) = (h(x)) * (h(y));$$

it also respects the inverse law $\overline{*}$

$$\forall x, y \in G: \quad h(x \mathbin{\overline{*}} y) = (h(x)) \mathbin{\overline{*}} (h(y))$$

In fact

$$\begin{aligned} h(x \mathbin{\overline{*}} y) &= h(x * \bar{y}) && \text{(definition of } \overline{*}) \\ &= h(x) * h(\bar{y}) && (h \text{ is a homomorphism}) \\ &= h(x) * \overline{h(y)} && \text{(by (b))} \\ &= h(x) \mathbin{\overline{*}} h(y) && \text{(definition of } \overline{*}) \end{aligned}$$

(d) To establish that hG is a subgroup of $H, *$ it is sufficient to prove that

$$\forall u, v \in hG: \quad u \mathbin{\overline{*}} v \in hG$$

Since $u \in hG$, there exists $x \in G$ such that $u = h(x)$. Similarly, there exists $y \in G$ such that $h(y) = v$. We have therefore

$$\begin{aligned} u \mathbin{\overline{*}} v &= (h(x)) \mathbin{\overline{*}} (h(y)) \\ &= h(x \mathbin{\overline{*}} y) && \text{(by (c))} \end{aligned}$$

which establishes the assertion.

Exercises

1. Let $h : G, * \to H, *$ be a group homomorphism. If S is a subgroup of $G, *$, the image hS of S by h is a subgroup of $H, *$.

2. Consider the group $R[x], +$ of polynomials in x with real coefficients and let $r(p)$ be the remainder after division of the polynomial $p \in R[x]$ by $x^2 + 1$. The map

$$r : R[x] \to R[x] : p \to r(p)$$

is a homomorphism $R[x], + \to R[x], +$ (and thus an endomorphism of $R[x], +$). The reader is asked to describe its image.

3. As an application of exercise 1, show that the rotations about a fixed point 0 expressed in grades by the rationals modulo 1 form a group.

4. Every cyclic group is the image of $Z, +$ by a homomorphism.

5. (a) The homomorphic image of every cyclic group is a cyclic group.

(b) Let h be a homomorphism defined on the cyclic group grp (g). Show that h is determined by the image of a generating element of grp (g).

6. Every infinite cyclic group is isomorphic to Z, $+$.

7. Every finite cyclic group of order n is isomorphic to Z_n, $+$.

8. Find

(a) a homomorphism $Z_8, + \to Z_4, +$;
(b) a homomorphism $Z_8, + \to Z_2, +$;
(c) a homomorphism $Z_8, + \to \{0\}, +$;
(d) a homomorphism $Z_8, + \to \{1\}, ..$

The reader is asked to describe the images.

§5. A REMINDER OF SOME SET-THEORY NOTATIONS

Let

$$h : G, * \to H, *$$

be a homomorphism of groups.

The homomorphism h is first and foremost a map $G \to H$. Conforming to set-theory notations, we shall denote by hA the image by h of every subset A of G.

In symbols

$$\forall A \subset G: \qquad hA = \{h(a) \mid a \in A\}$$

For every subset B of H, we shall denote by $h^{-1}B$ the image of B by the inverse relation h^{-1}.

Putting this precisely

$$\forall B \subset H: \qquad h^{-1}B = \{x \in G \mid h(x) \in B\}$$

Warning: in order to facilitate writing we often omit brackets when no confusion can occur. Thus we shall simply write $h^{-1}hx$ and $i^{-1}hx$ instead of $h^{-1}\{h(x)\}$ and $i^{-1}(h(x))$.

Exercises

(We assume throughout that h is a homomorphism $G, * \to H, *$.)

1. $h^{-1}hx$ is the set of elements of G which have the same image as x by the homomorphism h.

The set $\{h^{-1}hx \mid x \in G\}$ is a partition of G which we call the quotient of G by h and which we denote by G/h.

2. The inverse image $h^{-1}S$ of every subgroup S of H, $*$ is a subgroup of G, $*$.

3. We have just seen that the elements of G/h are maximal sets of elements of G having the same image by h. Also $h^{-1}hx \to hx$ defines an injection $G/h \to H$ and a bifunction $G/h \to hG$.

This is the *canonical bifunction* between the quotient G/h of G by h and the image hG of G by h.

4. Let p be the projection of the plane Π onto the straight line $A \subset \Pi$ by means of lines parallel to the straight line P (which is not parallel to A). We have $p\Pi = A$ and Π/p is the set of projecting lines.

§6. THE QUOTIENT OF A HOMOMORPHISM

Let

$$h : G, * \to H, *$$

be a homomorphism of groups.

We know that there exists a bifunction i which maps the quotient G/h onto the image hG.

$$i : G/h \to hG : h^{-1}hx \to hx$$

The inverse relation i^{-1} is therefore a bifunction

$$i^{-1} : hG \to G/h : y \to h^{-1}y$$

Since hG is a subgroup of H, $*$, the bifunction i^{-1} allows us to carry over the structure of hG, $*$ onto G/h. We again denote by $*$ the group law thus defined on G/h, and the group $G/h, *$ is called the quotient group of G, $*$ by the homomorphism h.

Let us describe explicitly the law $*$ of G/h. Any elements of G/h may always be written $h^{-1}hx$ and $h^{-1}hy$ with $x, y \in G$. To calculate $h^{-1}hx * h^{-1}hy$, note that $h^{-1}hx$ is none other than the image of hx by i^{-1}.

Thus

$$i^{-1}hx = h^{-1}hx$$

and

$$i^{-1}hy = h^{-1}hy$$

Since i^{-1} is an isomorphism $hG, * \to G/h, *$, we must have

$$i^{-1}(hx * hy) = i^{-1}hx * i^{-1}hy$$

hence $$h^{-1}(hx * hy) = h^{-1}hx * h^{-1}hy$$

The law $*$ in $G/h, *$ is therefore defined by

$$\boxed{h^{-1}hx * h^{-1}hy = h^{-1}(hx * hy)}$$

Since h is a homomorphism we may replace $hx * hy$ in this formula by $h(x * y)$, which permits us to enunciate finally

$$\boxed{\begin{array}{c}\text{the law in } G/h, * \text{ is defined by} \\ h^{-1}hx * h^{-1}hy = h^{-1}h(x * y)\end{array}}$$

This expression of the law in G/h reveals that the projection

$$G \to G/h : x \to h^{-1}hx$$

is an epimorphism.

§7. THE HOMOMORPHISM THEOREM

The results obtained in §6 allow us to enunciate the

Theorem – Every homomorphism of groups

$$h : G, * \to H, *$$

is the composite

$$h = m \circ i \circ e$$

of the epimorphism

$$e : G, * \to G/h, * : x \to h^{-1}hx,$$

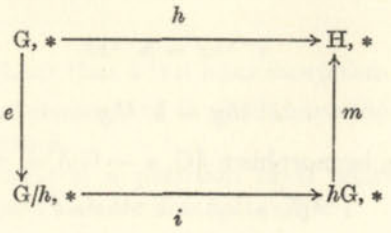
the isomorphism

$$i : G/h, * \to hG, * : h^{-1}hx \to hx,$$

and the monomorphism

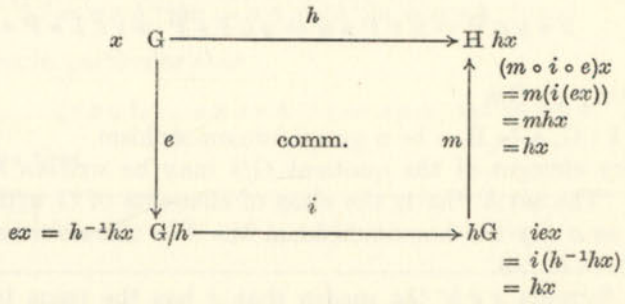
$$m : hG, * \to H, * : y \to y$$

This important theorem may be restated by saying that the following diagram is commutative.



The arrows in the above diagram indicate two possible routes for going from G to H. By saying that the diagram is commutative, we simply mean that, starting from an element x of G, we arrive at the same element of H whichever route we follow.

We indicate this below as a revision exercise.



§8. THE LAW INDUCED ON THE SET OF SUBSETS OF A GROUP

Let A and B be subsets of the group G, $*$. By definition, we put $A * B = \{a * b \mid a \in A, b \in B\}$. The set $\mathscr{P}G$ of subsets of G is thus provided with a law again denoted by $*$ which we sometimes call the law induced by the group law of G, $*$ in the set $\mathscr{P}G$.

If $a \in G$ and $B \subset G$ we shall write $a * B = \{a\} * B$ and $B * a = B * \{a\}$.

Exercises

1. The law $*$ of $\mathscr{P}G$ is associative.

2. If the group G is commutative, the law $*$ defined in $\mathscr{P}G$ is commutative.

3. The structure $\mathscr{P}G, *$ is not a group. (We note that, since $G, *$ is a group, $G \neq \varnothing$).

4. S is a stable subset of the group G, $*$ if and only if $S * S \subset S$.

5. If S is a subgroup of the group G, $*$, we have $S * S = S$. But we can have $S * S = S$ without S being a subgroup.

6. If A, B, C are subsets of G, $*$, the inclusion $B \subset C$ implies $A * B \subset A * C$ and $B * A \subset C * A$.

7. If s is an element of the subgroup S of G, $*$, we have

$$s * S = S * s = S$$

8. If A, B are subsets and x, y elements of the group G, $*$, we have

$$x * \mathrm{A} * y \subset \mathrm{B} \Leftrightarrow \mathrm{A} \subset \bar{x} * \mathrm{B} * \bar{y}$$

9. If x, y denote elements of a group G, $*$ and P a subset of this group

$$x * y \in \mathrm{P} \Leftrightarrow x \in \mathrm{P} * \bar{y} \Leftrightarrow y \in \bar{x} * \mathrm{P} \Leftrightarrow \nu \in \bar{x} * \mathrm{P} * \bar{y}$$

§9. STUDY OF G/h

Let $h : \mathrm{G}, * \to \mathrm{H}, *$ be a group homomorphism.

Every element of the quotient G/h may be written $h^{-1}ha$ with $a \in \mathrm{G}$. The set $h^{-1}ha$ is the class of elements of G with the same image as a (by the homomorphism h). We therefore have in particular $a \in h^{-1}ha$.

The formula $x \in h^{-1}ha$ means that x has the same image as a. It is equivalent to the formula $a \in h^{-1}hx$, which affirms that a has the same image as x. These two formulae are again equivalent to $ha = hx$. This last also amounts to saying that the class of elements with the same image as a coincides with the class of elements with the same image as x, which is expressed by the formula $h^{-1}ha = h^{-1}hx$.

We make a note of these remarks:

$$ha = hx \Leftrightarrow x \in h^{-1}ha \Leftrightarrow a \in h^{-1}hx \Leftrightarrow h^{-1}ha = h^{-1}hx \qquad (1)$$

We shall also use other formulae equivalent to $hx = ha$.

$$\begin{aligned} hx = ha &\Leftrightarrow h\bar{a} * hx = h\bar{a} * ha && \text{(since H, } * \text{ is a group)} \\ &\Leftrightarrow h(\bar{a} * x) = \nu && \text{(since } h \text{ is a homomorphism)} \\ &\Leftrightarrow \bar{a} * x \in h^{-1}\nu && \text{(definition of } h^{-1}\text{)} \\ &\Leftrightarrow x \in a * h^{-1}\nu && \text{(since G, } * \text{ is a group)} \end{aligned}$$

In the preceding reasoning we may interchange the rôles of a and x and multiply on the right instead of multiplying on the left.

We get

$$hx = ha \Leftrightarrow x \in a * h^{-1}\nu \Leftrightarrow x \in h^{-1}\nu * a \Leftrightarrow a \in h^{-1}\nu * x \Leftrightarrow a \in x * h^{-1}\nu \qquad (2)$$

Let us recapitulate the different ways of saying that a and x have the same image.

$$\begin{aligned} & hx = ha \\ \Leftrightarrow\ & h^{-1}hx = h^{-1}ha \\ \Leftrightarrow\ & x \in h^{-1}ha \Leftrightarrow x \in a * h^{-1}\nu \Leftrightarrow x \in h^{-1}\nu * a \\ \Leftrightarrow\ & a \in h^{-1}hx \Leftrightarrow a \in x * h^{-1}\nu \Leftrightarrow a \in h^{-1}\nu * x \end{aligned}$$

We stress in particular that

$$\forall a \in \mathrm{G}: \quad (\forall x \in \mathrm{G}: \quad x \in a * h^{-1}\nu \Leftrightarrow x \in h^{-1}ha \Leftrightarrow x \in h^{-1}\nu * a)$$

It follows that

$$\forall a \in \mathrm{G}: \quad a * h^{-1}\nu = h^{-1}ha = h^{-1}\nu * a \qquad (3)$$

Kernel

The set $h^{-1}\nu$ is called the kernel of the homomorphism h.

We see at once that this kernel is a subgroup of G, $*$. In fact,

$$x, y \in h^{-1}\nu \Leftrightarrow hx = hy = \nu$$

therefore

$$h(x \bar{*} y) = hx \bar{*} hy = \nu \bar{*} \nu = \nu$$

Q.E.D.

We have just seen (3) that the subgroup $h^{-1}\nu$ commutes with every element of G.

Normal subgroup

A subgroup S of G, $*$ is normal if and only if it commutes with every element of G, i.e. if and only if

$$\forall g \in \mathrm{G}: \quad g * \mathrm{S} = \mathrm{S} * g$$

A subgroup is therefore normal if and only if the left coset of every element coincides with its right coset.

Thus we can refer to the coset of an element for a normal subgroup without specifying whether it is a left coset or a right coset.

Theorem – The kernel of the group homomorphism $h : \mathrm{G}, * \to \mathrm{H}, *$ is a normal subgroup of G, *and the quotient group* G/h *is the set of cosets of the kernel.*

$$\mathrm{G}/h = \{h^{-1}ha \,\}\, a \in \mathrm{G}\} = \{a * h^{-1}\nu \,\}\, a \in \mathrm{G}\}$$

The group G/*h*, ∗, a substructure of $\mathscr{P}$G, ∗

We know that the law of G/*h*, ∗ has been defined unambiguously by

$$h^{-1}ha * h^{-1}hb = h^{-1}h(a * b)$$

Taking into account the results obtained above, this law can be rewritten

$$(a * h^{-1}\nu) * (b * h^{-1}\nu) = (a * b) * h^{-1}\nu$$

or if we prefer

$$(\{a\} * h^{-1}\nu) * (\{b\} * h^{-1}\nu) = (\{a\} * \{b\}) * h^{-1}\nu$$

A priori, this last formula is dangerous and hybrid. Indeed, the second sign ∗ is that of the law which has been defined in G/*h* (by the bifunction i^{-1}) while the other signs ∗ denote the law induced in $\mathscr{P}$G by the law of the group G, ∗.

In fact, if we interpret all the signs ∗ as expressions of the law in $\mathscr{P}$G, ∗, the preceding formula remains valid. In effect,

$$\begin{aligned}
&(\{a\} * h^{-1}\nu) * (\{b\} * h^{-1}\nu) \\
&\quad = \{a\} * (h^{-1}\nu * \{b\}) * h^{-1}\nu && \text{(associativity in } \mathscr{P}\text{G, ∗)} \\
&\quad = \{a\} * (\{b\} * h^{-1}\nu) * h^{-1}\nu && \text{(normality of } h^{-1}\nu\text{)} \\
&\quad = (\{a\} * \{b\}) * (h^{-1}\nu * h^{-1}\nu) && \text{(associativity in } \mathscr{P}\text{G, ∗)} \\
&\quad = (\{a\} * \{b\}) * h^{-1}\nu && \text{(since } h^{-1}\nu \text{ is a subgroup)}
\end{aligned}$$

Theorem – The quotient group G/*h*, ∗ *is a subgroup of the structure* $\mathscr{P}$G, ∗.

Exercises

1. A subgroup S of G, ∗ is normal if and only if $x * \mathrm{S} * \bar{x} \subset \mathrm{S}$ for every $x \in \mathrm{G}$.

2. All the subgroups of a commutative group are normal.

3. Find the normal subgroups of the symmetric groups $\mathscr{S}_2$, $\mathscr{S}_3$, $\mathscr{S}_4$.

4. If A is a normal subgroup and B a subgroup of the group G, ∗, the intersection A ∩ B is a normal subgroup of B.

5. The intersection of every set of normal subgroups of G, ∗, is a normal subgroup of G, ∗. We may therefore speak of the normal subgroup generated by every subset P of the group.

6. The neutral subgroup $\{\nu\}$ and the improper subgroup G are normal subgroups of G, ∗. A group $\neq\{\nu\}$ which does not admit normal subgroups other than its trivial subgroups is said to be *simple*.

7. If A is a normal subgroup and B a subgroup of the group G, ∗, then A ∗ B = B ∗ A is a subgroup of G, ∗.

8. Let A and B be subgroups of G, ∗ with A ⊂ B.

If A is a normal subgroup of G, ∗, it is *a fortiori* a normal subgroup of B.

If A is a normal subgroup of B and B a normal subgroup of G, A is not necessarily a normal subgroup of G.

Example: Let us consider $\mathscr{S}_4$, ∘, the symmetric group of degree 4.

The subgroup $\mathrm{V} = \left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$ is a normal subgroup of $\mathscr{S}_4$; sgp $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$ is in its turn a normal subgroup of the (commutative) group V, but it is not normal in $\mathscr{S}_4$.

9. The element g of the group G, ∗ defines the transformation of G

$$\mathrm{G} \to \mathrm{G} : x \to g * x * \bar{g}$$

This map is an automorphism of G, ∗. The automorphisms thus defined are called the inner automorphisms of G, ∗. A subgroup S is therefore normal if and only if it is stable for the inner automorphisms of G, ∗.

10. An element c of a group G, ∗ is said to be central if it commutes with every element of G, i.e. if we have

$$\forall g \in \mathrm{G}: \qquad c * g = g * c$$

The set of central elements of a group is called its centre.

The centre of a group is a normal subgroup.

Every subgroup included in the centre is called a central subgroup.

Every central subgroup is normal

The central elements of a group are the elements of this group which remain fixed under all the inner automorphisms.

Central subgroups are therefore not only stable for the inner automorphisms but remain fixed for the inner automorphisms (i.e. each of their elements is left fixed by the inner automorphisms).

11. The neutral element of the quotient group G/*h*, ∗ is the kernel $h^{-1}\nu$. By a new abuse of notation we shall sometimes denote it by ν.

The symmetric of the element $x * h^{-1}\nu$ is the element $\bar{x} * h^{-1}\nu$.

§10. THE QUOTIENT OF A GROUP BY A NORMAL SUBGROUP

We saw previously that the kernel $h^{-1}\nu$ of the group homomorphism $h : G, * \to H, *$ is a normal subgroup of G, $*$, and that knowledge of the kernel $h^{-1}\nu$ alone gives us the entire structure of the quotient group G/h, $*$, since:

$$\boxed{\begin{array}{c} G/h = \{g * h^{-1}\nu \,\}\, g \in G\} \\ (x * h^{-1}\nu) * (y * h^{-1}\nu) = (x * y) * h^{-1}\nu \end{array}}$$

We are going to show that the kernels of homomorphisms are not particular normal subgroups but that every normal subgroup is the kernel of a homomorphism.

Let S be a normal subgroup of the group G, $*$. In the same way as we can define G/h from $h^{-1}\nu$, we shall define a group starting from S.

We shall call such a group the quotient of G by S and we shall denote it by G/S. It is defined by

$$G/S = \{g * S \,\}\, g \in G\}$$

It remains to define the law in G/S. Since every element of G/S is a subset of G, the set G/S is a subset of $\mathscr{P}G$. We shall show that it is a stable subset of $\mathscr{P}G$, $*$, thus immediately providing G/S with the law $*$.

Let $x * S$ and $y * S$ be two elements of G/S which we shall rewrite $\{x\} * S$ and $\{y\} * S$ so as to have to consider only the law of $\mathscr{P}G$, $*$. We must show that

$$(\{x\} * S) * (\{y\} * S) \in G/S$$

This is done by repeating the argument already given at the end of the preceding paragraph in the case of $h^{-1}\nu$.

$$\begin{array}{lll} (\{x\} * S) * (\{y\} * S) = \{x\} * (S * \{y\}) * S & & \text{(associativity in } \mathscr{P}G, *) \\ = \{x\} * (\{y\} * S) * S & & \text{(normality of S)} \\ = (\{x\} * \{y\}) * (S * S) & & \text{(associativity in } \mathscr{P}G, *) \\ = \{x * y\} * S & & \text{(because S is a subgroup)} \\ \in G/S & & \end{array}$$

Q.E.D.

We must prove that the structure G/S, $*$ we have just defined is a group.

The associativity of the law of G/S, $*$ derives from the associativity of the law of $\mathscr{P}G$, $*$.

The normal subgroup S is itself an element of G/S since $S = \nu * S \in G/S$.

We shall leave to the reader the task of verifying that S is the neutral element of G/S, $*$ and that $\bar{x} * S$ is a symmetric of $x * S$, thus proving the required result.

The projection $f : G \to G/S : x \to x * S$ is a homomorphism since

$$\begin{array}{lll} f(x * y) = (x * y) * S & & \text{(definition of } f) \\ = (x * S) * (y * S) & & \text{(the law in G/S, } *) \\ = f(x) * f(y) & & \text{(definition of } f) \end{array}$$

The kernel of this hormophism is clearly S.

Theorem – If S *is a normal subgroup of the group* G, $*$, *the set* $G/S = \{g * S \,\}\, g \in G\}$ *is a group for the law defined in* $\mathscr{P}G$ *by the law of* G, $*$. *The map* $G \to G/S : x \to x * S$ *is an epimorphism whose kernel is the normal subgroup* S.

Corollary. The quotient of a group G, $*$ by a homomorphism coincides with the quotient of this group by the kernel of the homomorphism.

In symbols: $G/h = G/h^{-1}\nu$.

Exercises

1. Let R be a relation defined in the set E and p a permutation of E.

The relation $p \circ R \circ p^{-1}$ is called the transform of R by p.

We have

$$p \circ R \circ p^{-1} = \{(py, px) \,\}\, (y, x) \in R\}$$

Illustrate this concept by a diagram.

2. Let A, B, C be straight lines of the plane Π such that B is the bisector of one of the angles AC. If we denote the symmetries defined by these lines by a, b, c respectively, then

$$b \circ a \circ b^{-1} = c$$

Knowing that a rotation is the product of two symmetries, what can you say about the transform of a rotation by a symmetry?

We call the subgroup of $\mathscr{S}\Pi$ generated by the symmetries of Π

the group of displacements and turnings or the group of isometries of the plane Π.

The translations form a normal subgroup of the group of isometries. The quotient group is isomorphic to the group generated by the symmetries, all of which leave the same point fixed.

3. Every homothety† and every translation of the plane is called a dilatation of the plane. The set of non-constant dilatations is a group for the product of composition. The set of translations is a normal subgroup of it, and the quotient group is isomorphic to the group of non-constant homotheties with fixed centre, and therefore also to R_0, ..

§11. FIRST ISOMORPHISM THEOREM (EMMY NOETHER)

Let B and S be normal subgroups of the group A, $*$ such that $S \subset B \subset A$. It is evident that S is a normal subgroup of B. We shall show that B/S is a normal subgroup of A/S and that the quotient (A/S)/(B/S) is isomorphic to A/B, which we write

$$\boxed{(A/S)/(B/S) \cong A/B}$$

Because of the homomorphism theorem, it is sufficient to exhibit an epimorphism

$$A/S \to A/B$$

whose kernel is precisely B/S.

Every element of A/S is of the form $a * S$ with $a \in A$ and this element defines without ambiguity

$$\begin{aligned} (a * S) * B &= a * (S * B) && \text{(associativity in } \mathscr{P}A, *) \\ &= a * B && \text{(since S is a subgroup of B)} \end{aligned}$$

It follows immediately that the map thus defined

$$f : A/S \to A/B : a * S \to a * B$$

is an epimorphism.

Since the neutral element of A/B is none other than B, the kernel of the epimorphism f is the set of $a * S$ such that $a * B = B$. Therefore

$$f^{-1}\nu = \{a * S \mid a * B = B\} = \{a * S \mid a \in B\} = \{b * S \mid b \in B\} = B/S$$

Q.E.D.

† Tr. Radial expansion or similarity. See Appendix.

Theorem – Let B *and* S *be normal subgroups of the group* A, $*$ *such that* $S \subset B \subset A$. *The quotient* B/S *is then a normal subgroup of* A/S, *and we have*

$$\boxed{(A/S)/(B/S) \cong A/B}$$

by the canonical isomorphism $(a * S) * B/S \to a * B$.

Exercises

1. Verify Emmy Noether's theorem in the case where

$$\begin{aligned} A &= Z, + \\ B &= 2Z, + \\ S &= 6Z, + \end{aligned}$$

2. Verify Emmy Noether's theorem in the case where

$$\begin{aligned} A &= Z_{60}, + \\ B &= Z_{15}, + \\ S &= Z_3, + \end{aligned}$$

3. Let A be the additive group of vectors starting from a fixed point 0 of ordinary space.

Let B be the subgroup of A formed by the vectors of A having their end-points in a fixed plane α passing through 0.

Let S be the subgroup of B formed by the vectors of B with their end-points on a fixed straight line d, such that $d \subset \alpha$ and $0 \in d$.

Determine: A/S,
B/S,
(A/S)/(B/S),
A/B.

§12. SECOND ISOMORPHISM THEOREM

Let A be a subgroup and B a normal subgroup of the group G, $*$. The normality of B implies $A * B = B * A$ and it is easy to see that $A * B = B * A$ is a subgroup of G, $*$. We therefore have

$$B \subset A * B = B * A \subset G$$

and B is a normal subgroup of $A * B$. (The reader should note that this result is in fact the only hypothesis required in the subsequent reasoning.)

We shall show that $A \cap B$ is a normal subgroup of A and that

$$\boxed{A/(A \cap B) \cong (A * B)/B}$$

To establish this isomorphism, it is sufficient, on account of the homomorphism theorem, to exhibit an epimorphism $f : A \to (A * B)/B$ whose kernel is precisely $A \cap B$.

Since $A \subset A * B$, the identical map is a homomorphism of A into $A * B$. Composing this homomorphism with the canonical homomorphism $A * B \to (A * B)/B$ we obtain a homomorphism $A \to (A * B)/B$ defined by

$$\begin{array}{ccccc} A & \to & A * B & \to & (A * B)/B \\ a & \to & a & \to & a * B \end{array}$$

Note that

$$\begin{aligned} (A * B)/B &= \{(a * b) * B \mid a \in A, b \in B\} \\ &= \{a * B \mid a \in A\} \end{aligned}$$

This shows that the homomorphism

$$f : A \to (A * B)/B : a \to a * B$$

is an epimorphism.

Since the neuter of $(A * B)/B$ is none other than B, the kernel of the epimorphism f is the set of $a \in A$ such that $a * B = B$. Thus

$$\begin{aligned} \text{Kernel } f &= \{a \in A \mid a * B = B\} \\ &= \{a \in A \mid a \in B\} \qquad \text{(since B is a subgroup)} \\ &= A \cap B \end{aligned}$$

Q.E.D.

Theorem – Let A *be a subgroup and* B *a normal subgroup of the group* G, $*$; *the intersection* $A \cap B$ *is then a normal subgroup of* A *while* B *is a normal subgroup of the group* $A * B = B * A$. *We have moreover* $A/(A \cap B) \cong (A * B)/B$ *by the canonical isomorphism* $a * (A \cap B) \to a * B$.

Exercises

1. Consider the cyclic group of 24 elements generated by a:

$$\{0, a, 2a, 3a, \ldots, 23a\}, +$$

Verify the second isomorphism by taking A = grp $(3a)$, B = grp $(4a)$.

2. Do the same for $G = Z_{60}, +$
$A = Z_{12}, +$
$B = Z_4, +$

3. Let G be the additive group of vectors starting from a fixed point 0 of ordinary space;
let A be the subgroup of G whose elements are the vectors of G with their end-points in a fixed plane α containing 0;
let B be the subgroup of G whose elements are the vectors of G with their end-points in a fixed plane β containing 0.
Determine: $A/(A \cap B)$ and $(A + B)/B$.

Revision exercises on Chapter 7

1. Let H be a subgroup of the group G, $*$. Let us define for the moment

$$\forall x, y \in G: \qquad x \equiv y \text{ (modulo H)} \Leftrightarrow \bar{x} * y \in H$$

Prove:

(1) this relation is an equivalence
(2) $x \equiv y$ (mod H) $\Leftrightarrow x$ and y are in the same ... coset.
(3) $x \equiv y$ (mod H) $\Rightarrow \forall g \in G: \quad g * x \equiv g * y$ (mod H).
(4) $(x \equiv y$ (mod H) $\Rightarrow \forall g \in G: \quad x * g \equiv y * g$ (mod H)
$\Leftrightarrow$ (H is a normal subgroup of G).

2. Modify propositions (2), (3), (4) by taking the definition

$$\forall x, y \in G: \qquad x \equiv y \text{ (modulo H)} \Leftrightarrow x * \bar{y} \in H$$

3. The map

$$Z, + \to C_0, . : x \to i^x$$

is a group homomorphism.

4. The map

$$R, + \to C_0, . : x \to e^{ix}$$

is a group homomorphism. What is its kernel?

5. For every integer $z \in Z$, the map $e^{i\theta} \to e^{i\theta z}$ is an endomorphism of the group $\{\exp i\theta \mid \theta \in R\}, .$. What is the kernel of this endomorphism? What is the image? Determine the intersection of the kernel and the image.

6. Prove that Z, + is isomorphic to the multiplicative group $\{2^z \mid z \in Z\}, .$.

7. (a) Prove that $\{2^a 3^b \mid a, b \in Z\}, .$ is a subgroup of $Q_0, .$.
(b) This subgroup is isomorphic to the subgroup

$\{a + bi \mid a, b \in Z\}, +$ of C, +,
(it is sufficient to prove that
$\{a + bi \mid a, b \in Z\}, + \to \{2^a 3^b \mid a, b \in Z\} : a + bi \to 2^a 3^b$
is an isomorphism).

8. The groups C, + and $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in R\right\}, +$ are isomorphic groups.

9. The groups $C_0, .$ and $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in R, \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}, .$ are isomorphic groups.

10. The group of transformations $R \to R : x \to ax + b$, with $a \neq 0$ is isomorphic to the group $R_0 \times R, *$, where $*$ is defined by

$$\forall (a, b), (c, d) \in R_0 \times R: \qquad (a, b) * (c, d) = (ac, bc + d)$$

11. Let

$$\mathfrak{M} = \left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in R \text{ and } ad \neq 0\right\}.$$

(a) $\mathfrak{M}, .$ is a group.

(b) $\mathfrak{M}, . \to R_0, . : \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \to a$ is a group homomorphism.

12. Let $R \oplus R, +$ be a group† (where: $(a, b) + (c, d) = (a + c, b + d)$). Prove that the map

$$R \oplus R, + \to R, + : (x, y) \to x$$

is a homomorphism. What is the kernel? What is the image?

13. What is the subgroup generated by a non-identical translation in the group of translations of space? To what standard group is this group isomorphic?

14. The map $Z \to R/Z : z \to \frac{z}{4}$ is a homomorphism. It is neither a monomorphism, nor an epimorphism. The map $z \to \frac{z}{4}$ is an epimorphism of Z, + onto Z_4, +.

† Tr. $R \oplus R = \{(a, b) \mid a, b \in R\}$ See Revision exercises on Chs. 1 & 2, Ex. 28.

15. Let $i : G, * \to H, *$ be a group isomorphism. Prove that the order of every element of G is equal to the order of its image.

16. (a) The set of integers {1, 2, 3, 4} forms a group of order 4 for multiplication modulo 5, defined by

$$\forall a, b \in \{1, 2, 3, 4\}: \qquad a * b = r_5(a.b)$$

where r_5 denotes "the remainder after division by 5 of".
The set of integers {1, 3, 5, 7} forms a group of order 4 for multiplication modulo 8.
These two groups of order 4 are not isomorphic as is shown by their multiplication tables.

.mod 5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

.mod 8	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

In the second group every element is of order 2; on the other hand, in the first we have $2.2 = 4 \neq 1$ and $3.3 = 4 \neq 1$. These two groups are therefore not isomorphic (see Exercise 15).
(b) The set of integers {1, 3, 7, 9} provided with the product modulo 10 is a group of order 4. To which of the two groups of (a) is it isomorphic?
The same problem for the group of order 4 formed by the set of integers {1, 5, 7, 11} provided with the product modulo 12.
(c) Indicate the groups isomorphic to Z_4, + among the groups considered in (a) and (b). Do the same for Klein's four-group.

17. Is the multiplicative group {1, 5, 8, 12}, . mod 13 isomorphic to the multiplicative group {1, 5, 7, 11}, . mod 12?

18. Prove that—up to isomorphism—there are only two groups of order 4: the cyclic group with 4 elements and Klein's four-group.

19. Show that the group of 8 elements defined in exercise 45 of Chapter 2 is not isomorphic to the quaternion group.

20. The set of integers {1, 2, 4, 7, 8, 11, 13, 14} forms a group of order 8 for multiplication modulo 15. Is this group isomorphic to

the quaternion group or to the group $Z_4 \oplus Z_2, +$? (it is sufficient to write down three Cayley tables).

21. The following groups are all isomorphic to Klein's four-group.

(a) the group $\mathscr{P}\{a, b\}, \Delta$;

(b) the subgroup of $\mathscr{S}_4, \circ$ generated by the subset

$$\left\{\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\right\}$$

(c) the direct sum $Z_2 \oplus Z_2, +$ where the law is defined, we recall, by

$$\forall (a, b), (c, d) \in Z_2 \oplus Z_2: \qquad (a, b) + (c, d) = (a + c, b + d).$$

(d) the group of permutations f_1, f_2, f_3, f_4 of R_0

$$\begin{aligned} f_1 &: R_0 \to R_0 : x \to x, \\ f_2 &: R_0 \to R_0 : x \to 1/x, \\ f_3 &: R_0 \to R_0 : x \to -x, \\ f_4 &: R_0 \to R_0 : x \to 1/x. \end{aligned}$$

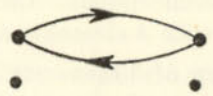
(e) the group of permutations which conserve the cross-ratio of four points (explanation: let a_1, a_2, a_3, a_4 be four points in a straight line; we say that the permutation φ of $\{1, 2, 3, 4\}$ conserves the cross-ratio (a_1, a_2, a_3, a_4) when $(a_{\varphi 1}\, a_{\varphi 2}\, a_{\varphi 3}\, a_{\varphi 4}) = (a_1\, a_2\, a_3\, a_4)$).

(f) the set formed by the identical permutation and the symmetries of space with respect to the edges of a trihedral trirectangle (provided with the law $\circ$).

(g) the multiplicative group formed by the matrices

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}-1&0\\0&-1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}0&-1\\-1&0\end{pmatrix}$$

(h) the subgroup of $\mathscr{S}_4, \circ$ which conserves the relation defined by the diagram



(explanation: $p \in \mathscr{S}_4$ conserves the relation R when $a\,R\,b \Leftrightarrow pa\,R\,pb$).

22. The following groups are isomorphic to the cyclic group of order 6.

(a) the subgroup of $\mathscr{S}_5, \circ$ generated by the element

$$\begin{pmatrix}1&2&3&4&5\\2&1&4&5&3\end{pmatrix},$$

(b) the subgroup of $\mathscr{S}_6, \circ$ generated by the element

$$\begin{pmatrix}1&2&3&4&5&6\\2&3&4&5&6&1\end{pmatrix},$$

(c) the direct sum $Z_2 \oplus Z_3, +$

(d) the multiplicative group of 6th roots of unity.

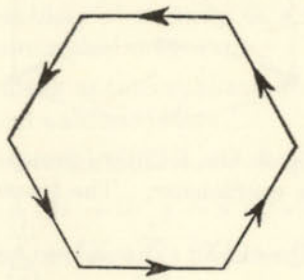
(e) the multiplicative group of 6 matrices

$$\left\{\begin{pmatrix}\cos(\pi/3)&\sin(\pi/3)\\-\sin(\pi/3)&\cos(\pi/3)\end{pmatrix}, \begin{pmatrix}\cos(2\pi/3)&\sin(2\pi/3)\\-\sin(2\pi/3)&\cos(2\pi/3)\end{pmatrix},\right.$$

$$\begin{pmatrix}\cos\pi&\sin\pi\\-\sin\pi&\cos\pi\end{pmatrix}, \begin{pmatrix}\cos(4\pi/3)&\sin(4\pi/3)\\-\sin(4\pi/3)&\cos(4\pi/3)\end{pmatrix},$$

$$\left.\begin{pmatrix}\cos(5\pi/3)&\sin(5\pi/3)\\-\sin(5\pi/3)&\cos(5\pi/3)\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}$$

(f) the subgroup of $\mathscr{S}_6, \circ$ which conserves the relation



(g) the group of integers $\{1, 2, 3, 4, 5, 6\}, .$ mod 7;

(h) the group of integers $\{1, 2, 4, 5, 7, 8\}, .$ mod 9.

23. The following groups are isomorphic to the symmetric group $\mathscr{S}_3, \circ$.

(a) the subgroup of $\mathscr{S}_3, \circ$ generated by the subset

$$\left\{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\};$$

(b) the subgroup of the symmetric group of $\{1, 2, 3, 4\}$ which leaves the element 1 fixed.

(c) the group of 6 functions $R \setminus \{0, 1\} \to R \setminus \{0, 1\}$

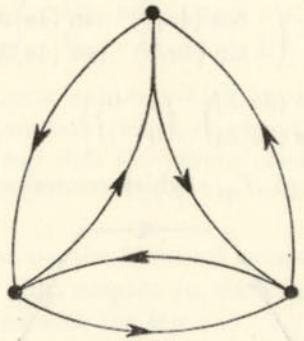
$$f_1 : R \setminus \{0, 1\} \to R \setminus \{0, 1\} : x \to x,$$
$$f_2 : R \setminus \{0, 1\} \to R \setminus \{0, 1\} : x \to 1/x,$$
$$f_3 : R \setminus \{0, 1\} \to R \setminus \{0, 1\} : x \to 1 - x,$$
$$f_4 : R \setminus \{0, 1\} \to R \setminus \{0, 1\} : x \to 1 - 1/x,$$
$$f_5 : R \setminus \{0, 1\} \to R \setminus \{0, 1\} : x \to 1/(1 - x),$$
$$f_6 : R \setminus \{0, 1\} \to R \setminus \{0, 1\} : x \to -x/(1 - x).$$

(d) the multiplicative group of six matrices

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}\alpha & 0\\ 0 & \alpha^2\end{pmatrix}, \begin{pmatrix}\alpha^2 & 0\\ 0 & \alpha\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & \alpha^2\\ \alpha & 0\end{pmatrix}, \begin{pmatrix}0 & \alpha\\ \alpha^2 & 0\end{pmatrix}\right\},$$

where α is a non-real cubic root of 1;

(e) the subgroup of $\mathscr{S}_3$ conserving the relation



24. Denote by $C[X], +$ the additive group of polynomials in the letter X with complex coefficients. The transformation

$$d : C[X] \to C[X] : \sum_{i=0}^{n} a_i X^i \to \sum_{i=1}^{n} i a_i X^{i-1}$$

is an endomorphism of $C[X], +$.
Determine: $d^{-1}0$, $dC[X]$, $d^{-1}0 \cap dC[X]$.

25. The reader is asked to give many examples of endomorphisms of groups and to determine in each case the kernel, the image and the intersection of the kernel and the image.

26. Let $G, +$ be a commutative group. For every $z \in Z$, the map $G \to G : g \to zg$ is an endomorphism of G (see Chapter 3).

27. For every $z_1 \in Z$, the map $Z \to Z : z \to z_1 z$ is an endomorphism of the infinite cyclic group $Z, +$. Prove that every endomorphism of $Z, +$ is of this form.

28. For every $q_1 \in Q$, the map $Q \to Q : q \to q_1 q$ is an endomorphism of $Q, +$. Prove that every endomorphism of $Q, +$ is of this form.

29. For every non-null rational q_1, the map $Q \to Q : q \to q_1 q$ is an automorphism of $Q, +$. Prove that every automorphism of $Q, +$ is of this form.

30. Let $G, .$ be a commutative (multiplicative) group. For every $z \in Z$, the map

$$G \to G : g \to g^z$$

is an endomorphism of G (see Chapter 3).

31. Find a homomorphism of the multiplicative group of invertible $n \times n$ matrices with real elements onto $R_0, .$.

32. Let $G, *$ be a group; let a be a fixed element of G. The map

$$a : G \to G : g \to a * g * \bar{a} = a \,.\, g$$

is an automorphism of the group G (which we call the inner automorphism of G defined by a).

33. Prove that the set of inner automorphisms of a group $G, *$ forms a subgroup of the group of automorphisms of G.

34. Every automorphism of a group $G, *$ transforms every subgroup of G into an isomorphic subgroup.

35. The group of inner automorphisms of a commutative group reduces to the identical automorphism.

36. The inner automorphism of $G, *$ defined by the element $a \in G$

$$a : G \to G : g \to a * g * \bar{a}$$

is the identical automorphism of G if and only if a is an element of the centre of G.

37. The group of automorphisms of a finite group is finite.

38. Let $G, *$ be a group. Prove that the map $G \to G : x \to \bar{x}$ is an automorphism of G if and only if G is a commutative group.

39. (a) The map

$$R \to R : x \to -x$$

is an automorphism of the group $R, +$.

(b) The map

$$R_0 \to R_0 : x \to -x$$

is not an endomorphism of the group $R_0, .$.

40. (a) The map

$$C \to C : a + bi \to a - bi$$

is an automorphism of the group C, +.

(b) The map

$$C_0 \to C_0 : a + bi \to a - bi$$

is an automorphism (not inner) of the group $C_0, .$.

41. Let V be the additive group of vectors with origin 0 of ordinary space. Let Π be a plane containing 0. Prove that symmetry with respect to Π is an automorphism of V, +.

42. Let G, $*$ be a group.

(a) The image by every endomorphism of G of a generating subset of G is a generating subset of the image of G.

(b) The image by every automorphism of G of a generating subset of G is a generating subset of G.

43. Look for the group of automorphisms of the infinite cyclic group Z, + (see preceding exercise). Construct the Cayley table of this group of automorphisms.

44. Find the groups of automorphisms of the following finite cyclic groups (see Ex. 42).

(a) Z_2, +
(b) Z_3, +
(c) Z_4, +
(d) Z_5, +
(e) Z_6, +
(f) Z_7, +
(g) Z_8, +
(h) Z_{10}, +
(i) Z_{11}, +
(j) Z_{12}, +
(k) Z_p, + with p prime.

In each case construct a Cayley table. Are there any different cyclic groups having isomorphic groups of automorphisms?

45. (a) Find the group of automorphisms of Klein's four-group.

(b) Do the same for $\mathscr{S}_3$, the symmetric group of degree 3.

46. By studying the preceding exercises, can you reply to the following three questions:

(a) Can two non-isomorphic groups have isomorphic groups of automorphisms?

(b) Can the group of automorphisms of a commutative group be non-commutative?

(c) Can the group of automorphisms of an infinite group be finite?

47. The automorphism of Klein's four-group defined by $a \to b$, $b \to a$ (where $\{a, b\}$ is a generating subset of V) is an outer automorphism.†

48. Is the automorphism of the quaternion group defined by $i \to j, j \to i$ inner?

49. Consider the additive cyclic group of order n generated by a. Prove that the endomorphism of grp (a) defined by grp $(a) \to$ grp (a) : $a \to ma$ $(0 \leqslant m < n)$ is an automorphism if and only if $m \wedge n = 1$.

50. Prove that all the automorphisms of $\mathscr{S}_3$ are inner automorphisms.

51. Prove that the group of inner automorphisms of a group G, $*$ is a normal subgroup of the group of all the automorphisms of G, $*$.

52. Is the set of transformations $R \to R : x \to x + b$ with $b \in R$ a normal subgroup of the group of transformations

$$R \to R : x \to ax + b, \quad \text{with } 0 \neq a, b \in R?$$

53. The map of the group of transformations $R \to R : x \to ax + b$ (with $0 \neq a, b \in R$) onto $R_0, .$ which sends the map $x \to ax + b$ onto the non-null real number a is a group homomorphism. Determine its kernel.

54. Every subgroup of index 2 is normal.

55. Is the subgroup $\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\}$ of $\mathscr{S}_3$ normal?

56. Is the subgroup

$$V = \left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$$

(isomorphic to Klein's four-group) of $\mathscr{S}_4$ normal?

† Tr. Any automorphism which is not an inner automorphism is called an outer automorphism.

57. Prove that all the subgroups of the quaternion group are normal subgroups (we express this fact by saying that the quaternion group is hamiltonian).

58. Denote by $GL_n(R)$ the set of $n \times n$ real invertible matrices. Prove

(a) $GL_n(R)$ is a group for the matrix product.

(b) The matrices of determinant 1 form a normal subgroup of $GL_n(R)$.

59. Let G, $*$ be a group. Prove that if $P \in \mathscr{P}G$ and N is a normal subgroup of G, then $P * N = N * P$.

60. Let $\mathfrak{M}$, $\subset$ be the ordered set of normal subgroups of a group G, $*$.

(1) $\mathfrak{M}$, $\subset$, $\cap$, $*$ is a lattice.

(2) this lattice is modular.†

Résumé: The lattice of normal subgroups of every group is modular.

61. Let $h : G, * \to H, *$ be a group homomorphism. If S is a normal subgroup of G, $*$, the image hS of S by h is a normal subgroup of hG, $*$.

62. Let $h : G, * \to H, *$ be a group homomorphism. The inverse image $h^{-1}S$ of every normal subgroup S is a normal subgroup of G.

63. Let G, $*$ and H, $*$ be two isomorphic groups. Prove that there exists a bifunction of the set of isomorphisms $G \to H$ onto the set of automorphisms of G.

64. A subgroup H of the group G, $*$ is normal if and only if it is stable for all the inner automorphisms of G (i.e. if and only if for every inner automorphism $a.$ of G we have $a.H \subset H$).

65. Every subgroup of G, $*$ which is stable for all the automorphisms of G is called a *characteristic subgroup* of G, $*$.

Every characteristic subgroup of a group is normal.

66. Every subgroup of G, $*$ which is stable for all the endomorphisms of G is called an *endostable* subgroup of G, $*$.

Every endostable subgroup of a group is characteristic (and therefore normal).

67. Let A and B be subgroups of G, $*$ such that $A \subset B$.

We know that if A is a normal subgroup of B and B a normal

† Tr. i.e. $A \subset C$ always implies $A \cup (B \cap C) = (A \cup B) \cap C$.

subgroup of G, the subgroup A is not always a normal subgroup of G (see Example, §9, Ex. 8).

Prove that if A is a characteristic (endostable resp.) subgroup of B and B a characteristic (endostable resp.) subgroup of G, then A is a characteristic (endostable resp.) subgroup of G.

68. The intersection of every family of characteristic subgroups of a group is characteristic.

69. The intersection of every family of endostable subgroups of a group is endostable.

70. The subgroup of a group generated by the union of a family of characteristic subgroups is characteristic.

71. The subgroup of a group G generated by the union of a family of endostable subgroups of G is an endostable subgroup of G.

72. Every group not identically null contains two endostable subgroups.

73. Every subgroup of a cyclic group is endostable.

74. Let G, $*$ be a group; let $z_0 \in Z$. Prove that

$$\operatorname{sgp} \{z_0 \perp g \} g \in G\}$$

is an endostable subgroup of G, $*$.

75. Let G, $*$ be a group. Prove that the set of elements of finite order of G is an endostable subgroup of G called the *periodic* subgroup of G.

76. Prove that the centre of a group is a characteristic subgroup.

77. Give a counter-example to show that the centre of a group is not always an endostable subgroup.

78. Every quotient of a cyclic group is cyclic.

79. The quotient of the cyclic group Z_4, $+$ by its subgroup of order 2 is isomorphic to Z_2 (note: $Z_4/Z_2 \cong Z_2$).

80. The quotient of Klein's four-group by any one of the three subgroups of order 2 is isomorphic to Z_2 (note: $V/Z_2 \cong Z_2$).

81. The quotient of the cyclic group Z_6, $+$ by its subgroup of order 3 is isomorphic to Z_2 (note: $Z_6/Z_3 \cong Z_2$).

82. (a) Prove that the set of permutations

$$\mathcal{A}_3 = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$$

is an invariant† subgroup of $\mathcal{S}_3$.
(b) $\mathcal{S}_3/\mathcal{A}_3 \cong \ldots$?

83. (a) Find $Z_{\mathcal{Q}}$, the centre of the quaternion group $\mathcal{Q}$.
(b) $\mathcal{Q}/Z_{\mathcal{Q}} \cong \ldots$?

84. Construct the quotient of the multiplicative group $\{2^x 3^y 5^z\}$ $x, y, z \in Z\}$, . by the subgroup $\{2^z\} z \in Z\}$.

85. Construct the quotient of the group $GL_n(R)$ by the normal subgroup of $n \times n$ matrices of determinant 1 (see Ex. 58).

86. Prove that the quotient of $\mathcal{S}_4$ by the invariant† subgroup

$$V = \left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}$$

is isomorphic to $\mathcal{S}_3$.

87. (a) Prove that the quotient of every group G by its centre Z_G is isomorphic to the group of inner automorphisms of G (it is sufficient to prove that the map h of G into the group of inner automorphisms of G which makes the inner automorphism $a.$ correspond to every $a \in G$ is an epimorphism and that the kernel of h is equal to Z_G).
(b) All the automorphisms of $\mathcal{S}_3$ are inner.

88. A group is cyclic if and only if it is isomorphic to a quotient of the infinite cyclic group Z, +.

89. Determine all the quotients of the cyclic group of order 24.

90. Find a homomorphism $\mathcal{S}_4 \to \mathcal{S}_3$. Determine the normal subgroup N of $\mathcal{S}_4$ such that $\mathcal{S}_4/N \cong \mathcal{S}_3$.

91. Describe
C_0/R_0, .
R_0/Q_0, .
C_0/Q_0, .

92. The derived group of a group.
Let G, $*$ be a group.
(a) For every $(x, y) \in G \times G$ the element $\bar{x} * \bar{y} * x * y$ of G is

† Tr. A normal subgroup is sometimes called an invariant subgroup.

called the *commutator* of x and y, and we denote it by $[x, y]$. Show that $\forall x, y \in G \times G$ we have

$x * y = y * x * [x, y]$,
$[x, y] * [y, x] = \nu$,
$\overline{[x, y]} = [y, x]$
$[x, \bar{y}] = y * [y, x] * \bar{y}$
$[\bar{x}, y] = x * [y, x] * \bar{x}$

The law $G \times G \to G : (x, y) \to [x, y]$ is not in general associative.
(b) In general the set of commutators of G, $*$ is not a subgroup of G.
(c) The subgroup of G generated by the set of commutators of G is called the derived group (or commutator group) of G and we denote it by G'. The subgroup G' is endostable (prove that the image of every commutator of G by every endomorphism of G is a commutator of G).
(d) The derived group of a commutative group is. . . .
(e) The derived group of a non-commutative simple group is. . . .
(f) Let $h : G, * \to H, *$ be a group homomorphism. Prove that $hG, *$ is a commutative subgroup of H if and only if $h^{-1}\nu \supset G'$.
(g) The quotient group G/K of a group G is commutative if and only if $K \supset G'$ (an immediate consequence of (f)).

93. What is the derived group of Klein's four-group?

94. Look for the derived group of the symmetric group $\mathcal{S}_3$. Find also $(\mathcal{S}_3)' = \mathcal{S}_3''$, $(\mathcal{S}_3'')' = \mathcal{S}_3'''$, $(\mathcal{S}_3''')' = \mathcal{S}_3''''$.

95. The same problem for the group $\mathcal{S}_4$, $\circ$.

96. Let $\mathcal{Q}$, . be the quaternion group. Find $\mathcal{Q}'$, $\mathcal{Q}''$, $\mathcal{Q}'''$, $\mathcal{Q}''''$.

97. Let H be a subgroup of the group G, $*$. Prove that $H' \subset G'$.

98. Prove that G'', G''', G'''', . . . are endostable subgroups of G (see Ex. 67 and 92, (c)).

99. Every subgroup H of the group G, $*$ containing G' is normal.

100. Every homomorphism h of a group G into a commutative group H is the composite of an epimorphism $G \to G/G'$, and a homomorphism $G/G' \to H$ (apply the first isomorphism theorem).

101. For every group G, $*$ we have $G' = \{\nu\} \Leftrightarrow G = Z_G$.

102. Give an example of a group G whose centre reduces to the neutral element and such that $G' \neq G$.

103. Give an example of a group G such that $G = G'$ and such that the centre of G does not reduce to the neutral element.

104. Compare the centre of the quaternion group with the derived group of the quaternion group.

105. Use exercises 1 to 104 to make numerous applications of the isomorphism theorems.

106. Let G, + be a commutative group. Denote by Endo (G, +) the set of endomorphisms of G, +. Endo G may be provided with two laws:

(1) a law +: for every pair (f, g) of endomorphisms of G we define $f + g$ as being the transformation

$$f + g : G \to G : x \to f(x) + g(x) \text{ of } G$$

(2) the product of composition, defined, let us recall, by

$$\forall f, g \in \text{Endo } G, \forall x \in G: \qquad (f \circ g)(x) = f(g(x))$$

Prove that Endo (G, +), +, $\circ$ is a ring. Hence: the set of endomorphisms of a commutative group is a ring.

107. Write down the addition and multiplication tables of the ring of endomorphisms of the four-group.

108. The ring of endomorphisms of the group Z, + is isomorphic to the ring Z, +, .; that is to say, there exists a bifunction

$$f : \text{Endo } (Z, +) \to Z,$$

such that

$$\forall h_1, h_2 \in \text{Endo } Z: \qquad f(h_1 + h_2) = f(h_1) + f(h_2)$$
$$\text{and} \qquad f(h_1 \circ h_2) = f(h_1) . f(h_2)$$

109. Exact sequences of groups.

Algebraic topology makes intensive use of certain algebraic ideas and of the subtle mechanics of cleverly arranged homomorphisms. To this effect, the topologists have introduced a new technique, that of exact sequences.

A sequence of groups and homomorphisms of groups

$$\ldots \xrightarrow{h_{i-2}} G_{i-1} \xrightarrow{h_{i-1}} G_i \xrightarrow{h_i} G_{i+1} \xrightarrow{h_{i+1}} \ldots \qquad (1)$$

is said to be exact at G_i when

$$h_{i-1}G_{i-1} = h_i^{-1}\nu$$

The sequence (1) is said to be exact when it is exact at each of its groups (with the exception of the first and the last). Sequence (1) is therefore exact when for every i the image of the $(i - 1)$th homomorphism is equal to the kernel of the ith.

Examples

(1) If $i : 2Z \to Z$ is the canonical monomorphism of 2Z into Z and if j is the canonical epimorphism $Z \to Z_2$, the sequence

$$\{0\} \longrightarrow 2Z \xrightarrow{i} Z \xrightarrow{j} Z_2 \longrightarrow \{0\}$$

is exact.

(2) More generally, let H be a normal subgroup of the group G, $*$ and denote by i the canonical monomorphism $H \to G$ and by j the canonical epimorphism $G \to G/H$.

The homomorphism theorem tells us that the sequence

$$\{\nu\} \longrightarrow H \xrightarrow{i} G \xrightarrow{j} G/H \longrightarrow \{\nu\}$$

is exact.

(3) Let us regard every point x of ordinary space E as the vector with fixed origin 0 and end-point x. The space E then appears as an additive group. Let D and P be a straight line and a plane such that $P \cap D = \{0\}$.

According to our conventions P and D are then subgroups of E.

Denote by p the projection of E on D parallel to P and by d the projection of E on P parallel to D. The transformations p and d of E are endomorphisms of E and the sequence

$$\ldots \xrightarrow{d} E \xrightarrow{p} E \xrightarrow{d} E \xrightarrow{p} E \xrightarrow{d} E \xrightarrow{p} \ldots$$

is exact.

110. Let $h : A, * \to B, *$ be a group homomorphism.

The sequence $\{\nu\} \to A \xrightarrow{h} B$ is exact if and only if h is a monomorphism.

The sequence $A \xrightarrow{h} B \to \{\nu\}$ is exact if and only if h is an epimorphism.

The sequence $\{\nu\} \to A \xrightarrow{h} B \to \{\nu\}$ is exact if and only if h is an isomorphism.

111. The sequence of groups and homomorphisms

$$\{\nu\} \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow \{\nu\}$$

is exact if and only if the following three conditions are simultaneously satisfied

(1) f is a monomorphism,
(2) g is an epimorphism,
(3) $f\,\mathrm{A} = g^{-1}(\nu)$.

If the given sequence is exact the group A is isomorphic to a normal subgroup of B and the group C is isomorphic to the quotient of B by a normal subgroup isomorphic to A.

8

Permutations

§1. DEFINITION (revision)

Let us remind ourselves that we call every relation f defined in a set E such that every element of E is the origin of one and only one pair of f and the end-point of one and only one pair of f a permutation of E.

Exercises

1. Every translation of the plane Π is a permutation of Π.

2. The symmetry of the plane Π with respect to a straight line A is a permutation of the plane Π.

3. Every non-constant homothety† of the plane Π is a permutation of Π.

4. Every rotation of the plane Π is a permutation of Π.

5. The identical map of a set E is a permutation of E.

6. The relation f defined in the set E is a permutation of E if and only if this is also so of its inverse f^{-1}.

7. If f and g are permutations of the set E so is the composite $g \circ f$.

8. If f is a permutation of E we have $f^{-1} \circ f = f \circ f^{-1} =$ the identical transformation of E.

9. The set $\mathscr{S}\mathrm{E}$ of permutations of the set E is a group for the product of composition. This group is called the symmetric group of E.

10. The function $f : \{a, b\} \to \{a, b\}$ with $a \neq b$ defined by $f(a) = b$ and $f(b) = a$ is called a *transposition* of the pair $\{a, b\}$, and we write it (a, b).

The reader should establish that (a, b) is a permutation of the set $\{a, b\}$.

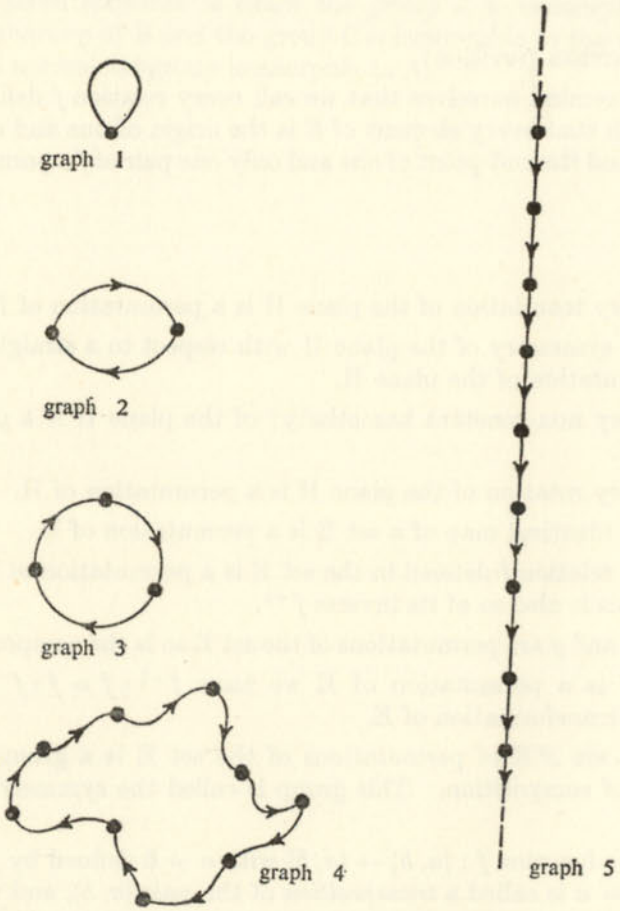
11. Let us remember that we call the set of origins of pairs of a

† Tr. See Appendix.

relation R the domain of R. We call the set of end-points of pairs of R the image of the relation R. The domain and the image of a relation R will be denoted by dom R and img R respectively.

If f is a permutation of the set E, we have $\mathrm{dom}\, f = \mathrm{img}\, f = \mathrm{E}$.

If $\mathrm{S} \subset \mathrm{R}$, we have $\mathrm{dom\, S} \subset \mathrm{dom\, R}$ and $\mathrm{img\, S} \subset \mathrm{img\, R}$.



12. If $\mathrm{E} \supset \{a, b\}$ with $a \neq b$ we also denote by (a, b) the permutation of E defined by

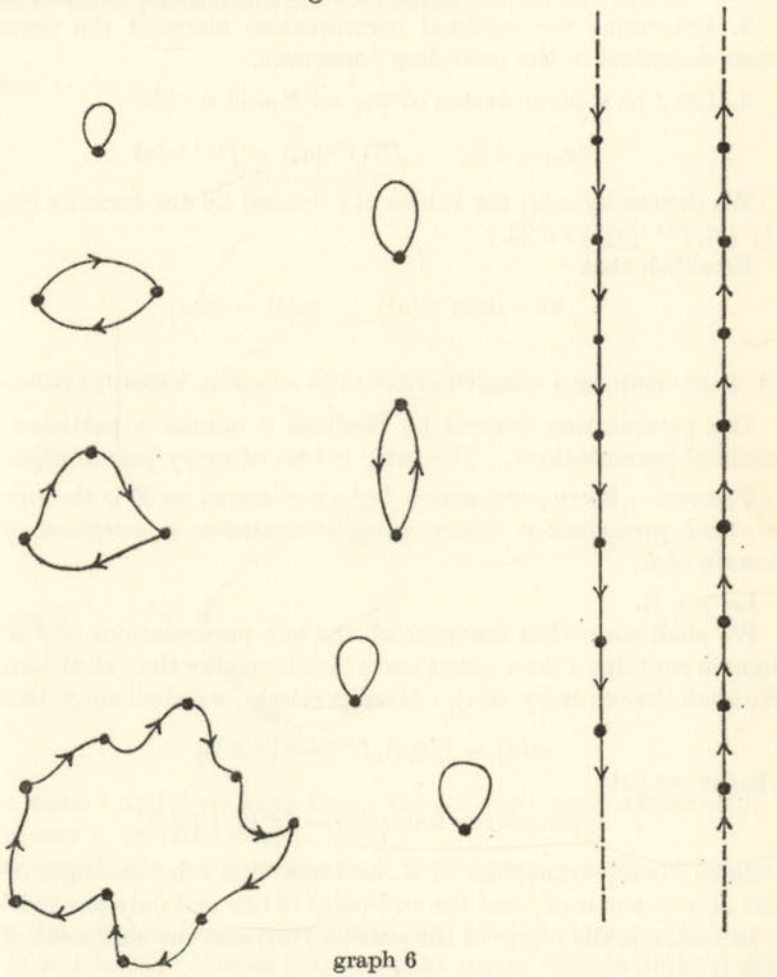
$$\mathrm{E} \to \mathrm{E} : \begin{cases} a \to b \\ b \to a \\ x \to x \text{ for every } x \in \mathrm{E} \setminus \{a, b\} \end{cases}$$

13. If f and g are permutations such that $g \subset f$, i.e. $\mathrm{dom}\, g \subset \mathrm{dom}\, f$, and the set of pairs of $g \subset$ the set of pairs of f, we say that g is a sub-permutation of f.

§2. MINIMAL PERMUTATIONS

The above diagrams represent permutations.

The same is true of the diagrams below.



graph 6

The permutation defined by diagram 6 contains proper sub-permutations while the permutations defined by diagrams 1 to 5 do not contain proper sub-permutations.

Definition. A permutation is minimal if and only if it does not contain a non-empty proper sub-permutation.

Exercises

1. The permutations defined by diagrams 1 to 5 are minimal; the permutation defined by diagram 6 is not minimal.

2. Determine the minimal permutations amongst the permutations described in the preceding paragraph.

3. Let f be a permutation of the set E and $a \in \mathrm{E}$.

$$\forall z_1, z_2 \in \mathrm{Z}: \qquad f^{z_1}(f^{z_2}(a)) = f^{z_1+z_2}(a)$$

We denote by $m(a)$ the subset of f defined by the formula $m(a) = \{(f^z(a), f^{z+1}(a)) \mid z \in \mathrm{Z}\}$.†

Establish that

$$\forall b \in \mathrm{dom}\ m(a): \qquad m(b) = m(a)$$

§3. PARTITION OF A PERMUTATION INTO MINIMAL PERMUTATIONS

The permutation defined by diagram 6 admits a partition into minimal permutations. The same is true of every permutation.

Theorem – Every permutation f of a non-empty set E *is the union of minimal permutations whose domains constitute a partition of the domain of f.*

Let $a \in \mathrm{E}$.

We shall show that amongst all the sub-permutations of f whose domain contains a there exists one which is smaller than all the others. We shall denote it by $m(a)$. More precisely, we shall show that

$$m(a) = \{f^z(a), f^{z+1}(a) \mid z \in \mathrm{Z}\} \tag{1}$$

whence we get

$$\mathrm{dom}\ m(a) = \mathrm{img}\ m(a) = \{f^z(a) \mid z \in \mathrm{Z}\} \tag{2}$$

Since f is a permutation of E, we know that a is the origin of one and only one pair of f and the end-point of one and only one pair of f.

In fact, a is the origin of the pair $(a, f(a))$ and the end-point of the pair $(f^{-1}(a), a)$.

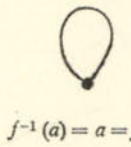
† Tr. $f^z(a) = \underbrace{f \circ f \circ \ldots \circ f}_{\text{2 terms}}, (a),$

Starting from the point a, we therefore consider the elements $f^{-1}(a)$ and $f(a)$. Three cases may arise:

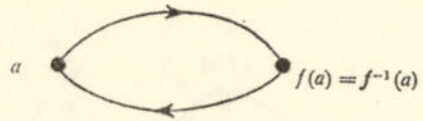
(1) $\quad f(a) = f^{-1}(a) = a$
(2) $\quad f(a) = f^{-1}(a) \neq a$
(3) $\quad a \neq f(a) \neq f^{-1}(a) \neq a$

These three possibilities are illustrated graphically below.

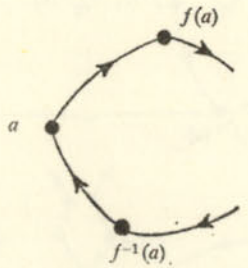
Case 1



Case 2



Case 3



In cases 1 and 2 we have found the required permutation $m(a)$.

In case 1, we have $m(a) = \{(a, a)\}$.

In case 2, the permutation $m(a)$ is the transposition of the pair $\{a, f(a)\}$.

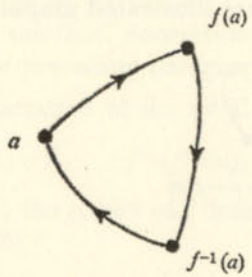
In the graphical representation of case 3 we have started the arrow (of f) which sets off from $f(a)$ and that which finishes off at $f^{-1}(a)$. Nothing has been assumed about the end-point of the arrow starting from $f(a)$ nor about the origin $f^{-2}(a)$ of the arrow with end-point $f^{-1}(a)$.

Three new possible cases arise:

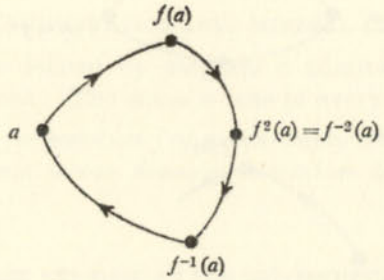
(3.1) $f^2(a) = f^{-1}(a)$ and $f^{-2}(a) = f(a)$.
(3.2) $f^2(a) = f^{-2}(a) \neq f^z(a)$ with $|z| < 2$.
(3.3) $f^2(a) \neq f^{-2}(a)$ and $f^2(a) \neq f^z(a) \neq f^{-2}(a)$ with $|z| < 2$.

These are represented graphically by

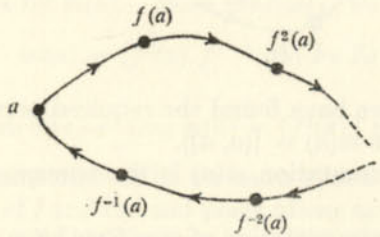
Case 3.1



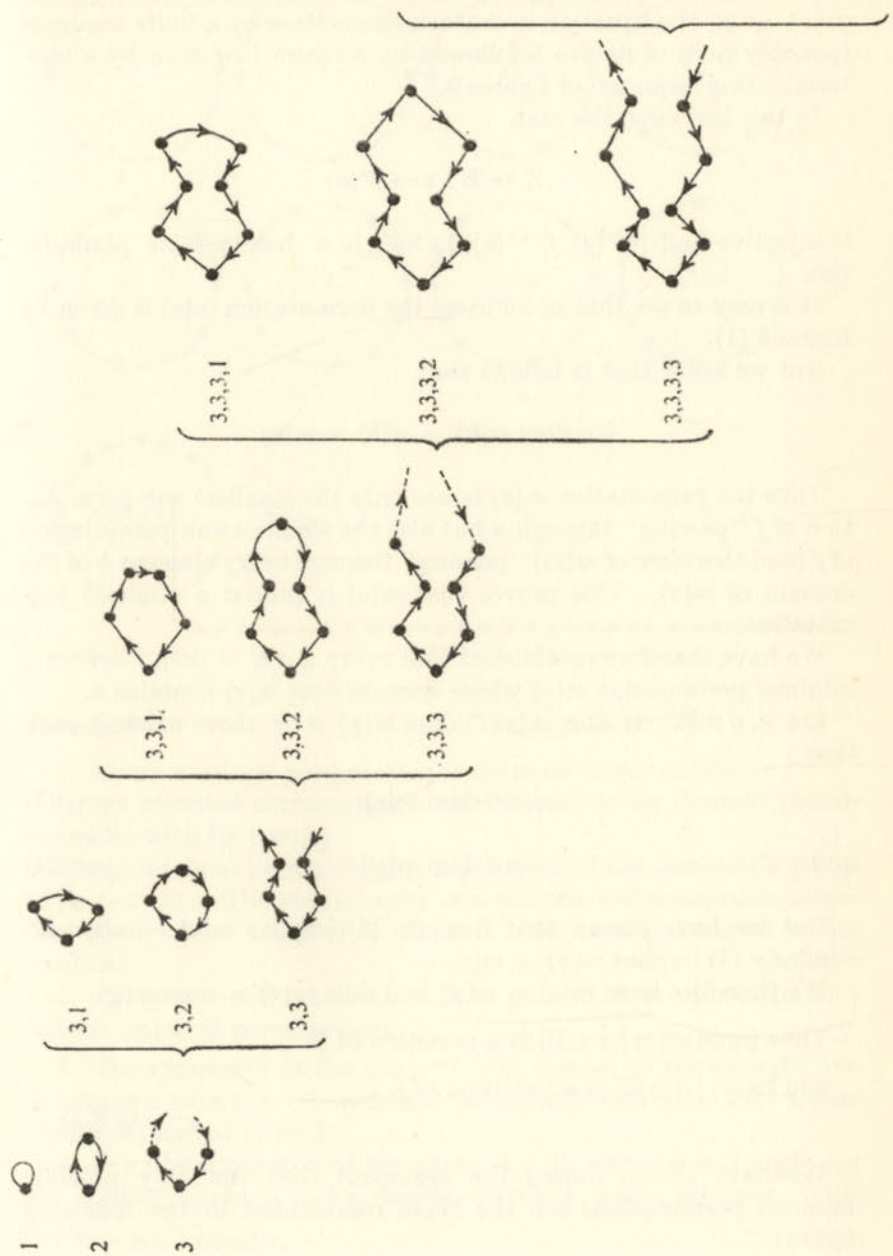
Case 3.2



Case 3.3



In cases 3.1 and 3.2 the problem is solved and $m(a)$ is then a permutation of a set of 3 or 4 elements respectively. In case 3.3 a new trichotomy arises. The steps in the continuation of our reasoning are illustrated schematically on the next page.



Whatever the permutation f defined on a set E and whatever the point $a \in \mathrm{E}$, the situation is characterized either by a finite sequence (possibly null) of figures 3 followed by a figure 1 or 2, or by a non-terminating sequence of figures 3.

In this last case, the map

$$\mathrm{Z} \to \mathrm{E} : z \to f^z(a)$$

is injective and $\{(f^z(a), f^{z+1}(a)) \mid z \in \mathrm{Z}\}$ is a denumerable permutation.

It is easy to see that in all cases the permutation $m(a)$ is given by formula (1).

But we know that it follows that

$$b \in \operatorname{dom} m(a) \Rightarrow m(b) = m(a)$$

Thus the permutation $m(a)$ is not only the smallest sub-permutation of f "passing" through a but also the smallest sub-permutation of f (and therefore of $m(a)$) "passing" through every element b of the domain of $m(a)$. This proves that $m(a)$ is indeed a minimal permutation.

We have therefore established that every $x \in \mathrm{E} = \operatorname{dom} f$ defines a minimal permutation $m(x)$ whose domain $\operatorname{dom} m(x)$ contains x.

Let $x, y \in \mathrm{E}$. If $\operatorname{dom} m(x) \cap \operatorname{dom} m(y) \neq \varnothing$ there exists z such that

$$z \in \operatorname{dom} m(x) \tag{3}$$

and

$$z \in \operatorname{dom} m(y) \tag{4}$$

But we have shown that formula (3) implies $m(x) = m(z)$ and similarly (4) implies $m(y) = m(z)$.

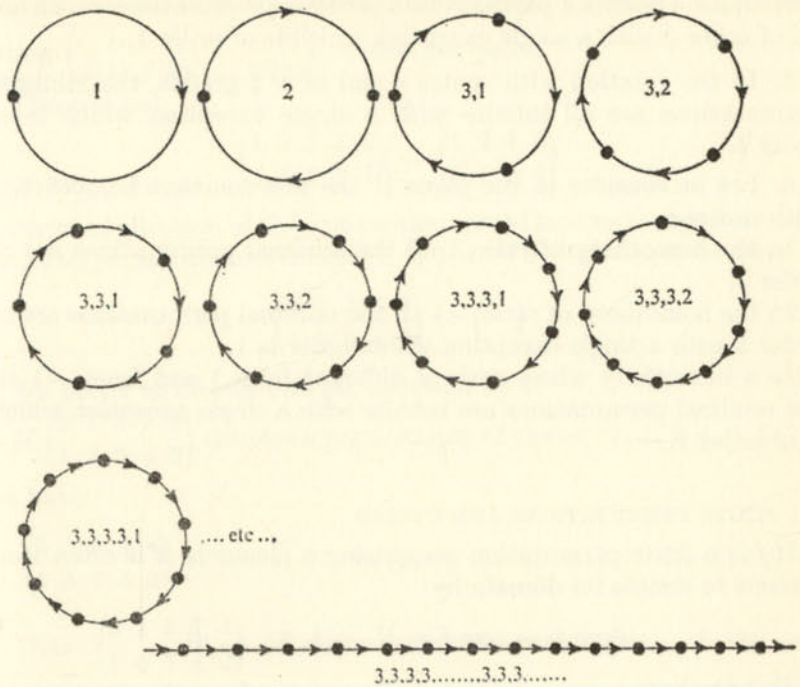
We therefore have $m(x) = m(y)$ and $\operatorname{dom} m(x) = \operatorname{dom} m(y)$.

Thus $\{\operatorname{dom} m(x) \mid x \in \mathrm{E}\}$ is a partition of E

and $\{m(x) \mid x \in \mathrm{E}\}$ is a partition of f.

Q.E.D.

We have shown during the argument that the only possible minimal permutations are the types represented in the following figure:



Exercises

1. Every minimal permutation is finite or denumerable.

Every minimal permutation is equipotent† to its domain (which coincides with its image).

Every minimal permutation is an element of the symmetric group of its domain. The idea of order of a minimal permutation is therefore clear. The order of a minimal permutation is equal to its cardinal.

2. Every non-null translation of the plane admits a partition into infinite minimal permutations.

3. The symmetry of the plane Π with respect to the straight line A admits a partition into minimal permutations of order 2 (or transpositions) and of order 1.

4. Let f be a rotation of the plane Π with centre 0 and angle p/q (in grades) where p and q denote mutually prime integers. This

† Tr. See Appendix.

permutation admits a partition into minimal permutations which are all of order q with a single exception which is of order 1.

5. In the rotation with centre c and of $\sqrt{2}$ grades, the minimal permutations are all infinite with a single exception which is of order 1.

6. Let us consider in the plane Π the non-constant homotheties with centre c.

In the homothety of ratio 1 all the minimal permutations are of order 1.

In the homothety of ratio -1 all the minimal permutations are of order 2 with a single exception whose order is 1.

In a homothety whose ratio is different from 1 and from -1 all the minimal permutations are infinite with a single exception which is of order 1.

§4. FINITE PERMUTATIONS AND CYCLES

If f is a finite permutation comprising n elements it is often convenient to denote its domain by

$$\operatorname{dom} f = \operatorname{img} f = \mathrm{N} = \{1, 2, \ldots, n\}$$

This implies

$$f = \{(1, f(1)), (2, f(2)), \ldots, (n, f(n))\}$$

which is also written

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$$

In this notation it is unnecessary to give precedence to any particular order for the first line. Thus we can also write

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 1 & 3 & 4 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 1 & 3 & 2 & 4 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

If p is a permutation of $\{1, 2, \ldots, n\}$, the permutation f may be written

$$f = \begin{pmatrix} 1, & 2, & \ldots, & n \\ f(1), f(2), & \ldots, & & f(n) \end{pmatrix} = \begin{pmatrix} p(1), & p(2), & \ldots, & p(n) \\ f(p(1)), f(p(2)), & \ldots, & & f(p(n)) \end{pmatrix}$$

Knowing that all the permutations considered involve the set

$\{1, 2, \ldots, n\}$ we allow ourselves to simplify the notation by amputating $\begin{pmatrix} 1, & 2, & \ldots, & n \\ f(1), f(2), & \ldots, & & f(n) \end{pmatrix}$ of identical pairs.

Thus we put

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 5 \\ 5 & 1 & 2 & 4 \end{pmatrix}$$

Strict application of this convention would lead us to represent the identical permutation of the set $\{1, 2, 3, 4, 5\}$ by "an empty bracket".

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} & \end{pmatrix}$$

We prefer to denote this permutation by I.

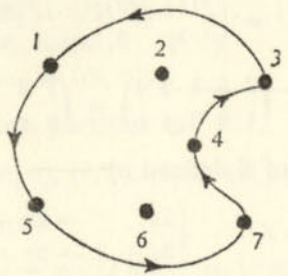
If $\begin{pmatrix} 3 & 1 & 5 & 7 & 4 \\ 1 & 5 & 7 & 4 & 3 \end{pmatrix}$ denotes a permutation of the set $\{1, 2, 3, 4, 5, 6, 7\}$, we have

$$\begin{pmatrix} 3 & 1 & 5 & 7 & 4 \\ 1 & 5 & 7 & 4 & 3 \end{pmatrix} = \{(4, 3), (7, 4), (5, 7), (1, 5), (3,1), (2, 2), (6, 6)\}.$$

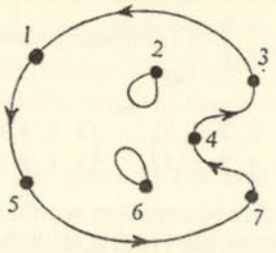
Thus $\begin{pmatrix} 3 & 1 & 5 & 7 & 4 \\ 1 & 5 & 7 & 4 & 3 \end{pmatrix}$ is not a minimal permutation of the set $\{1, 2, \ldots, 7\}$. It is the union of a minimal permutation of the set $\{1, 3, 4, 5, 7\}$ and of the identical permutation of the complementary set $\{2, 6\}$.

We shall define a cycle of the set E to be the union of a minimal permutation of a subset P of E and the identical permutation of $\mathrm{E} \setminus \mathrm{P}$.

The rather subtle difference between the concepts of minimal permutation and cycle is illustrated by the following diagram.



Minimal permutation of {1, 3, 4, 5, 7}



Cycle of {1, 2, 3, 4, 5, 6, 7}

Every cycle of N (distinct from the identical permutation) contains one and only one minimal permutation (distinct from the identical permutation) of a subset P of N.

Conversely, every minimal permutation of a subset P of N defines a cycle of N.

In order to simplify the notation we shall put

$$(3, 1, 5, 7, 4) = \begin{pmatrix} 3 & 1 & 5 & 7 & 4 \\ 1 & 5 & 7 & 4 & 3 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 3 & 7 & 6 & 4 \end{pmatrix}$$

$$= \{(7, 4), (5, 7), (1, 5), (3, 1), (4, 3), (2, 2), (6, 6)\}$$

This notation, which is in current use, is very convenient but incomplete since it does not indicate which set is permuted.

Exercises

1. If f is a permutation of $\{1, 2, \ldots, n\}$ we have

$$f^{-1} = \begin{pmatrix} f(1), f(2), \ldots, f(n) \\ 1, \quad 2, \quad \ldots, \quad n \end{pmatrix}$$

2. $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 5 & 1 & 2 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

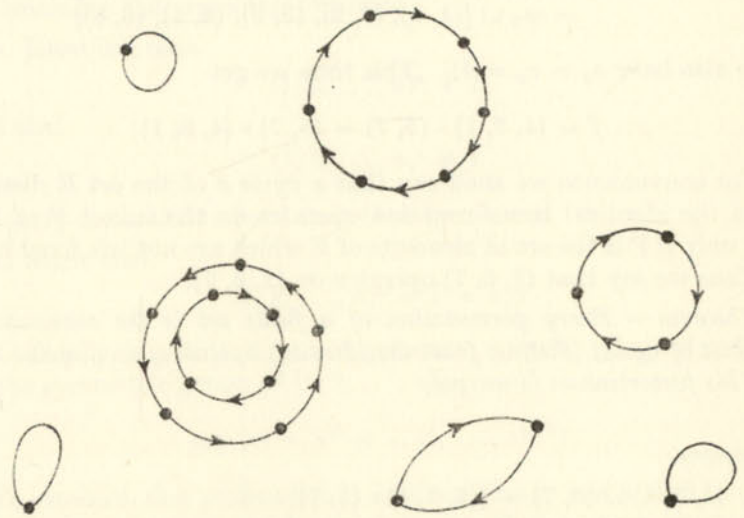
3. The permutation of Z defined by

$$\forall z \in \mathrm{Z}: \quad \begin{cases} 2z & \to 2z + 2 \\ 2z + 1 & \to 2z + 1 \end{cases}$$

is a cycle of Z. Draw its diagram.

§5. DECOMPOSITION OF A PERMUTATION OF A FINITE SET INTO CYCLES

We shall apply the theorem of partition of a permutation into minimal permutations to the case of finite sets. Such a permutation, comprising only a finite number of pairs, cannot admit infinite cycles. Also the diagram of a permutation of finite order must have the following appearance.



The minimal permutations of the permutation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 1 & 3 & 7 & 6 & 5 \end{pmatrix}$$

are

$$m_1 = \{(3, 1), (4, 3), (1, 4)\}$$
$$m_2 = \{(2, 2)\}$$
$$m_3 = \{(5, 7), (7, 5)\}$$
$$m_4 = \{(6, 6)\}$$

and $\{m_1, m_2, m_3, m_4\}$ is a partition of

$$f = \{(5, 7), (6, 6), (7, 5), (4, 3), (3, 1), (2, 2), (1, 4)\}$$

In particular we have

$$f = m_1 \cup m_2 \cup m_3 \cup m_4$$

Note that $m_1 \circ m_2 \circ m_3 \circ m_4 = \varnothing$ (1)

(We even have $m_i \circ m_j = \varnothing$ whenever $i \neq j$.)

Let us substitute for the non-identical minimal permutations the cycles which they define.

$$\begin{aligned} c_1 = (4, 3, 1) &= \{(1, 4), (3, 1), (4, 3), (2, 2), (5, 5), (6, 6), (7, 7)\} \\ &= m_1 \cup \{(2, 2), (5, 5), (6, 6), (7, 7)\} \\ c_3 = (5, 7) &= \{(7, 5), (5, 7), (1, 1), (2, 2), (3, 3), (4, 4), (6, 6)\} \\ &= m_3 \cup \{(1, 1), (2, 2), (3, 3), (4, 4), (6, 6)\} \end{aligned}$$

(We also have $c_2 = c_4 = \mathrm{I}$). This time we get

$$f = (4, 3, 1) \circ (5, 7) = (5, 7) \circ (4, 3, 1)$$

For convenience we shall say that a cycle c of the set E distinct from the identical transformation operates on the subset P of E if and only if P is the set of elements of E which are not left fixed by c.

Thus we say that (2, 5, 7) operates on {2, 5, 7}.

Theorem – Every permutation of a finite set is the commutative product of cycles (distinct from the identity) operating on disjoint sets. This factorization is unique.

Exercises

1. $(1, 3, 4) \cup (5, 7) = ((1, 3, 4) \circ (5, 7)) \cup \mathrm{I}$.

2. Note that the notation (5, 7) is ambiguous. It denotes on the one hand the pair with origin 5 and end-point 7 and on the other hand {(5, 7), (7, 5), (1, 1), (2, 2), (3, 3), (4, 4), (6, 6)}. As always when dealing with homonyms, only the context allows us to avoid confusion. The reader should note that if (5, 7) denotes the cyclic permutation, we have (5, 7) = (7, 5) while if (5, 7) denotes the pair, (5, 7) ≠ (7, 5).

3. Decompose into cycles the permutations:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 7 & 5 & 3 & 12 & 2 & 4 & 6 & 14 & 8 & 13 & 11 & 1 & 10 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 3 & 8 & 9 & 4 & 1 & 6 & 7 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 2 & 11 & 5 & 6 & 12 & 7 & 9 & 1 & 10 & 3 & 4 \end{pmatrix}$$

4. Establish the formulae:

$$\begin{aligned} (1, 2)^2 &= \mathrm{I} \\ (a, b)^2 &= \mathrm{I} \\ (1, 2, 3, 4)^2 &= (1, 3) \circ (2, 4) \\ (1, 2, 3, 4, 5, 6)^2 &= (1, 3, 5) \circ (2, 4, 6) \\ (1, 2, 3, 4, 5, 6)^3 &= (1, 4) \circ (2, 5) \circ (3, 6) \end{aligned}$$

Generalize the preceding formulae.

5. Establish that

$$(1, 2, \ldots, n)^n = \mathrm{I}$$

and that

$$(1, 2, \ldots, n)^t \neq \mathrm{I}$$

for every natural number t such that $1 \leqslant t < n$.

6. Show that

$$(1, 2, \ldots, n)^a = \mathrm{I} \Leftrightarrow n | a$$

7. The cycle $c = (1, 2, \ldots, n)$ generates a cyclic group of order n in the symmetric group of $\{1, 2, \ldots, n\}$.

$$\mathrm{grp}\,(c) = \{c^0 = 1, c^1, \ldots, c^{n-1}\}$$

To establish this proposition it only remains to verify that if a and b are distinct natural numbers strictly less than n, we have $c^a \neq c^b$. Assume $a < b$. By virtue of a preceding exercise we have $c^{b-a} \neq \mathrm{I}$, which establishes our proposition.

8. Establish the formula

$$(n, \ldots, 2, 1)^{-1} = (1, 2, \ldots, n) = (n, \ldots, 2, 1)^{n-1}$$

In particular

$$(b, a) = (b, a)^{-1}$$

9. Let $p = c_1 \circ c_2 \circ \ldots \circ c_s$ be the decomposition of the permutation p into non-identical cycles. The order of p is the L.C.M. of the orders of the c_i. We have

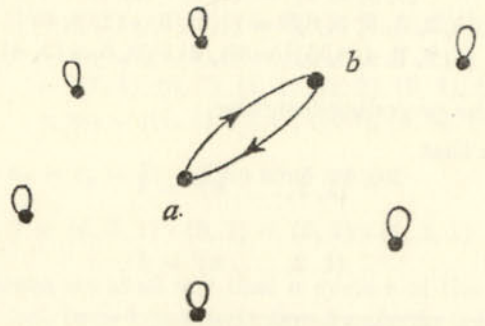
$$\forall k \in \mathrm{Z}: \qquad p^k = c_1^k \circ c_2^k \circ \ldots \circ c_s^k$$

In particular

$$p^{-1} = c_1^{-1} \circ c_2^{-1} \circ \ldots \circ c_s^{-1}$$

§6. DECOMPOSITION OF FINITE PERMUTATIONS INTO THE PRODUCT OF TRANSPOSITIONS

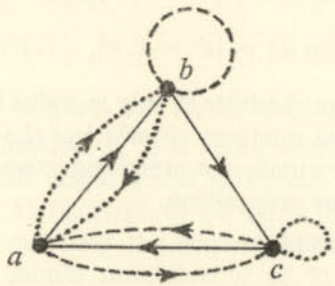
Every cycle of order 2, (a, b) with $a \neq b$, is called a transposition.



The cycle (b, a)

Every cycle decomposes into transpositions

$$(1, 2, 3, \ldots, n-1, n) = (1, n) \circ (1, n-1) \ldots \circ (1, 4) \circ (1, 3) \circ (1, 2).$$



$(a, c) \circ (a, b) = (a, b, c)$

Theorem – Every finite permutation decomposes into transpositions.

In effect, every permutation decomposes into cycles and every cycle decomposes into transpositions.

The decomposition of a permutation into transpositions is not unique:

$$\begin{aligned} I &= (2, 1) \circ (2, 1) = (3, 2) \circ (3, 2) = (2, 1) \circ (4, 3) \circ (2, 1) \circ (4, 3) \\ (1, 2, 3, 4) &= (4, 1) \circ (3, 1) \circ (2, 1) \\ &= (1, 2) \circ (4, 2) \circ (3, 2) \\ &= (1, 2) \circ (2, 3) \circ (3, 2) \circ (4, 2) \circ (3, 2) \end{aligned}$$

The number of transpositions which occur in the decomposition of a permutation is not unique. We shall prove that the parity of this number is determined by the permutation itself.

Proposition. Let p be a permutation and t a transposition of a finite set E. *The number of minimal permutations included in $p \circ t$ differs by unity from the number of minimal permutations included in p.*

Denote by $c(p)$ the number of minimal permutations (distinct or not from the identical permutation) contained in p.

We shall prove that

$$c(p \circ t) = c(p) \pm 1$$

Put

$$t = (a, b) \quad \text{with} \quad a, b \in \mathrm{E}$$

A priori there are two cases to consider.

1. a and b do not both belong to the domain of the same minimal permutation of p.

In this case the formula

$$(a, a_2, \ldots, a_w) \circ (b, b_2, \ldots, b_m) \circ (b, a) = (a, b_2, \ldots, b_m, b, a_2, \ldots, a_w) \quad (1)$$

shows that

$$c(p \circ t) = c(p) - 1$$

2. a and b both belong to the domain of the same minimal permutation of p.

Formula (1) again gives us

$$(a, b_2, \ldots, b_m, b, a_2, \ldots, a_w) \circ (b, a) = (a, a_2, \ldots, a_w) \circ (b, b_2, \ldots, b_m)$$

which establishes that in this case

$$c(p \circ t) = c(p) + 1$$

Q.E.D.

Theorem – If a permutation p is the product of an even number of transpositions, every decomposition of p into transpositions contains an even number of factors.

Corollary. The preceding enunciation remains valid when we substitute the word odd for the word even.

Let p be a permutation of a set E of n elements. Denote by $c(p)$ the number of minimal permutations contained in p, and let us consider the corresponding cycles.

Every cycle of order d admits a decomposition into $d - 1$ transpositions. Since the sum of the orders of the cycles of p is n, the permutation p admits a decomposition into a product of $n - c(p)$ transpositions.

Let

$$p = t_m \circ \ldots \circ t_1$$

be any decomposition of p into transpositions.

Then

$$p \circ t_1 \circ t_2 \circ \ldots \circ t_m = \mathrm{I}$$

Now

$$c(p \circ t_1 \circ t_2 \circ \ldots \circ t_m) = c(p) \underbrace{\pm 1 \pm 1 \pm 1 \ldots \pm 1}_{m}$$

and since $c(\mathrm{I}) = n$, we get

$$\underbrace{\pm 1 \pm 1 \pm 1 \ldots \pm 1}_{m} = n - c(p)$$

Thus the m terms of the left-hand side contain

$$(n - c(p)) \text{ terms equal to } 1$$

and, in addition, the term $+1$ the same number of times as the term -1.

Therefore the difference between m and $(n - c(p))$ is even.

Q.E.D.

Definition. A permutation is said to be even (odd resp.) if and only if it is composed of an even number (odd resp.) of transpositions.

Exercises

1. If $p = t_s \circ \ldots \circ t_1$ is a decomposition of the permutation p into transpositions, we have $p^{-1} = t_1 \circ \ldots \circ t_s$.

2. Decompose

$$\begin{pmatrix} 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 8 & 9 & 5 & 6 & 1 & 2 & 4 & 7 & 3 \end{pmatrix}$$

into transpositions.

3. Let $\mathrm{E} = \{1, \ldots, n\}$ be a finite set. The identical transformation of E is even.

4. Every transposition is odd.

5. The cycle (c, b, a) is even.

6. The cycle $(c_n, c_{n-1}, c_{n-2}, \ldots c_2, c_1)$ is even or odd according to whether n is odd or even.

7. The product of two even permutations is an even permutation.

8. The product of two odd permutations is an even permutation.

9. The product of an even permutation and an odd permutation is an odd permutation.

10. Every permutation is of the same parity as its inverse.

11. The set $\mathscr{A}_n$ of even permutations of the set $\mathrm{N} = \{1, \ldots, n\}$ is a subgroup of $\mathscr{S}_n$. We call it the alternating group of N.

§7. THE ALTERNATING GROUP

Definition. Let E *be a finite set. The group* $\mathscr{A}(\mathrm{E})$ *of even permutations of* E *is called the alternating group of* E.

We denote the alternating group of $\{1, \ldots, n\}$ *by* $\mathscr{A}_n$.

Theorem – The set $\mathscr{A}(\mathrm{E})$ *of even permutations of the finite set* E *is a normal subgroup of the symmetric group* $\mathscr{S}(\mathrm{E})$ *of this set.*

The quotient $\mathscr{S}(\mathrm{E})/\mathscr{A}(\mathrm{E})$ *is isomorphic to* Z_2.

1. Let $a \in \mathscr{A}(\mathrm{E})$ and $s \in \mathscr{S}(\mathrm{E})$.

Clearly we have $s \circ a \circ s^{-1} \in \mathscr{A}(\mathrm{E})$ (since s and s^{-1} have the same parity).

2. Since $\mathscr{A}(\mathrm{E})$ is the set of even permutations of E, the difference $\mathscr{S}(\mathrm{E}) \setminus \mathscr{A}(\mathrm{E})$ is the set of odd permutations.

The map

$$\mathscr{A}(\mathrm{E}) \to 0 \in \mathrm{Z}_2$$
$$\mathscr{S}(\mathrm{E}) \setminus \mathscr{A}(\mathrm{E}) \to \tfrac{1}{2} \in \mathrm{Z}_2$$

is an isomorphism

$$\mathscr{S}(\mathrm{E})/\mathscr{A}(\mathrm{E}), \circ \to \mathrm{Z}_2, +$$

Q.E.D.

Definition. A group $\neq \{v\}$ *is said to be simple if and only if it has no (non-trivial) normal subgroups.*

Theorem – The alternating group $\mathscr{A}_n$ *is simple for all* $n > 4$.

This theorem follows from the following lemmas.

LEMMA 1. Every even permutation is a product of ternary cycles.

(It is hardly necessary to mention that every cycle of order 3 is called a ternary cycle.)

Since an even permutation is the composite of an even number of transpositions, it is sufficient to prove that the product of two transpositions is a product of tricycles. This is established by the formulae

$$(b, a) \circ (b, a) = \mathrm{I} \text{ (product of the zero tricycle)}$$
$$(c, a) \circ (b, a) = (a, b, c)$$
$$(d, c) \circ (b, a) = (a, c, d) \circ (a, b, d)$$

LEMMA 2. Every normal subgroup H of $\mathscr{A}_n$ which contains a ternary cycle contains every ternary cycle.

Suppose that $(a, b, c) \in \mathrm{H}$ and let (i, j, k) be a ternary cycle of $\mathrm{N} = \{1, \ldots, n\}$.

We can always construct a permutation of N

$$\begin{pmatrix} a, b, c, \ldots \\ i, j, k, \ldots \end{pmatrix}$$

The lemma then follows from the formula

$$\begin{pmatrix} a, b, c, \ldots \\ i, j, k, \ldots \end{pmatrix} (a, b, c) \begin{pmatrix} a, b, c, \ldots \\ i, j, k, \ldots \end{pmatrix}^{-1} = (i, j, k)$$

LEMMA 3. Every normal subgroup of $\mathscr{A}_n$ which contains a ternary cycle is equal to $\mathscr{A}_n$.

An immediate consequence of lemmas 1 and 2.

LEMMA 4. If $n > 4$ every normal subgroup H of $\mathscr{A}_n$ different from the identical subgroup contains a ternary cycle.

We shall establish that the permutations of H which leave fixed the greatest number of elements of N are ternary cycles.

Let $p \in \mathrm{H}$ be a permutation of N which leaves fixed at least as many elements of N as every other permutation of H.

Suppose that p is not a ternary cycle, and consider the decomposition of p into cycles which are disjoint one from another.

If all the cycles of this decomposition are transpositions, then

$$p = (a, b) \circ (c, d) \circ \ldots \tag{1}$$

If not, one of the cycles is of order $\geqslant 3$ and

$$p = (a, b, c, \ldots) \circ \ldots \tag{2}$$

In this case there exists at least one element of $\mathrm{N} \setminus \{a, b, c\}$ which

is not left fixed by p. There must exist another element not left fixed by p since $\mathrm{H} \subset \mathscr{A}_n$. Denote these elements by e and f. Since $n \geqslant 5$, we can consider in both cases the ternary cycle $q = (c, e, f)$ (the elements a, b, c, e, f always being assumed distinct).

Let us transform p by q. According to whether we have (1) or (2) we get respectively

$$\begin{aligned} p_1 &= q \circ p \circ q^{-1} \\ &= (c, e, f) \circ (a, b) \circ (c, d) \circ \ldots \circ (c, e, f)^{-1} \\ p_1 &= (a, b) \circ (d, e) \circ \ldots \end{aligned} \tag{3}$$

and

$$\begin{aligned} p_1 &= q \circ p \circ q^{-1} \\ &= (c, e, f) \circ (a, b, c, \ldots) \circ \ldots \circ (c, e, f)^{-1} \\ &= (a, b, e, \ldots) \circ \ldots \end{aligned} \tag{4}$$

Since H is a normal subgroup, we have $p_1 \in \mathrm{H}$ and $p_1^{-1} \circ p \in \mathrm{H}$.

All the elements of $\mathrm{N} \setminus \{a, b, c, e, f\}$ left fixed by the permutation p are also left fixed by $p_1^{-1} \circ p$.

In the first case none of the elements a, b, c, d is left fixed by p. But

$$(p_1^{-1} \circ p)(a) = a \quad \text{and} \quad (p_1^{-1} \circ p)(b) = b$$

which proves that $p_1^{-1} \circ p$ leaves more elements fixed than p, contrary to hypothesis.

In the second case none of the elements a, b, c, e, f is left fixed by p.

But $(p_1^{-1} \circ p)(a) = a$, which again shows that $p_1^{-1} \circ p$ leaves fixed more elements than p.

It follows that p is a tricycle.

Q.E.D.

Revision exercises on Chapter 8

1. The symmetric groups of equipotent sets are isomorphic (clue: prove that if $b : \mathrm{E} \to \mathrm{F}$ is a bijection, $\mathscr{S}\mathrm{E}, \circ \to \mathscr{S}\mathrm{F}, \circ : f \to b \circ f \circ b^{-1}$ is an isomorphism.)

2. The transformation of Z defined by

$$\mathrm{Z} \to \mathrm{Z} : z \to z + 1$$

is a permutation of Z. Decompose it into cycles. Draw its diagram.

3. The transformation of R defined by

$$\mathrm{R} \to \mathrm{R} : x \to x^3$$

is a permutation of R.

4. Let G, $*$ be a group. The transformation of G defined by

$$G \to G : x \to \bar{x}$$

is a permutation of G. What is its decomposition into disjoint cycles? In what case is this permutation an automorphism?

5. Apply exercise 4 to the groups

$$Z, +; \quad Q_0, .; \quad Z_4, +$$

6. Decompose the following permutations into disjoint cycles.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 3 & 6 & 2 & 1 & 7 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 4 & 1 & 2 & 9 & 3 & 8 & 6 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 5 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 3 & 4 \end{pmatrix}$

(d) $(6, 5, 4, 3, 2, 1)^4$

7. Decompose all the elements of grp $\{(8, 7, 6, 5, 4, 3, 2, 1)\}$ into disjoint cycles.

8. Describe the partition of a translation of the plane into minimal permutations.

9. The same question for the symmetry of the plane with respect to the straight line A.

10. Important exercise

Let E be a set. For every n-cycle $(a_1, a_2, \ldots, a_n) \in \mathscr{S}E$ and for every $f \in \mathscr{S}E$, we have

$$f \circ (a_1, a_2, \ldots, a_n) \circ f^{-1} = (f(a_1), f(a_2), \ldots, f(a_n))$$

11. Find the cardinals of the symmetric groups of the following sets with cardinal $\leqslant 3$:

$$\begin{aligned} \#\mathscr{S}\varnothing &= 1 \\ \#\mathscr{S}_1 &= \ldots \\ \#\mathscr{S}_2 &= \ldots \\ \#\mathscr{S}_3 &= \ldots \end{aligned}$$

12. Let E be a finite set. We have

$$\#E = n \Rightarrow \#\mathscr{S}E = \ldots$$

13. The order of every permutation of $\{1, 2, \ldots, n\}$ divides $n!$

14. What are the commutative symmetric groups?

15. $\mathscr{S}_n$ contains subgroups isomorphic to $\mathscr{S}_m$ for every $m \leqslant n$.

16. (a) Which elements of $\mathscr{S}\{1, 2, 3, 4\}$ leave invariant the subset $\{1\}$ of $\{1, 2, 3, 4\}$?
(b) The same question for $\{1, 2\}$.
(c) The same for $\{1, 2, 3\}$.
(d) The same for $\{1, 2, 3, 4\}$.

17. Find $f, g \in \mathscr{S}_7$ such that

$$f \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 4 & 7 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 7 & 6 & 3 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 4 & 7 & 6 & 1 \end{pmatrix} \circ g$$

18. Give examples of

(a) even permutations of even order.
(b) even permutations of odd order.
(c) odd permutations of even order.
(d) odd permutations of odd order.

19. (a) Consider a cycle of order n. This cycle is even if and only if n is....
(b) If a product of cycles contains an even number of cycles of even order, it is even.

20. How many distinct k-cycles are there in $\mathscr{S}_n$?

21. Is the inverse of a cycle a cycle?

22. (a) What is the order of a k-cycle?
(b) Let $(a_k, \ldots, a_2, a_1)$, $(b_e, \ldots, b_2, b_1)$ be two cycles such that $\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_e\} = \varnothing$. Find the order of $(a_k, \ldots, a_2, a_1) \circ (b_e, \ldots, b_2, b_1)$.

23. Find a homomorphism of $\mathscr{S}_n, \circ$ onto the cyclic group of order 2. What is its kernel?

24. grp $\{(1, 2, 3)\} \circ$ grp $\{(2, 1)\}$ = grp $\{(2, 1)\} \circ$ grp $\{(1, 2, 3)\}$
grp $\{(2, 1)\} \circ$ grp $\{(3, 2)\} \neq$ grp $\{(3, 2)\} \circ$ grp $\{(2, 1)\}$

25. We have seen (§6) that the group $\mathscr{S}_n$ is generated by the set of

transpositions of $\{1, 2, \ldots, n\}$. Prove that the following subsets of $\mathscr{S}_n$ are also generating subsets of $\mathscr{S}_n$:

(a) $\{(1, 2), (1, 3), \ldots, (1, n)\}$;
(b) $\{(1, 2), (2, 3), \ldots, (n - 1, n)\}$;
(c) $\{(1, 2), (1, 2, 3, \ldots, n - 1, n)\}$;
(d) $\{(1, 2), (2, 3, 4, \ldots, n - 1, n)\}$.

26. Construct homomorphisms of $\mathscr{S}_4$ onto $\mathscr{S}_3$. In particular, construct three epimorphisms of $\mathscr{S}_4$ onto $\mathscr{S}_3$. In each case determine the kernel and the image.

27. Prove that in $\mathscr{S}_n$

$$\text{sgr}\,\{(1, 2, 3), (1, 2, 4), \ldots, (1, 2, n - 1), (1, 2, n)\} = \mathscr{A}_n$$

(clue: calculate $(1, 2, k) \circ (1, 2, k) \circ (1, 2, l) \circ (1, 2, k)$).

28. Prove that in $\mathscr{S}_n$

$$\text{sgr}\,\{(1, 2, 3), (3, 4, 5, \ldots, n - 1, n)\} = \mathscr{A}_n$$

29. grp $\{(2, 1) \circ (4, 3), (3, 1) \circ (4, 2)\}$ is isomorphic to Klein's four-group.

30. grp $\{(1, 2, 3, 4) \circ (5, 6, 7, 8), (1, 5, 3, 7) \circ (2, 8, 4, 6)\}$ is isomorphic to the quaternion group.

31. Let P be a group of permutations.

(a) If there exists an odd permutation in P, P contains as many even permutations as odd.
(b) The set of even permutations of P forms a subgroup of P.

32. Write down the multiplication table of

$$\text{grp}\,\{(2, 1), (3, 1) \circ (4, 2)\}$$

33. A permutation $\in \mathscr{S}_n$ commutes with $(1, 2, \ldots, n)$ if and only if it is a power of $(1, 2, \ldots, n)$.

34. Find the commutator of $(1, 2) \circ (3, 4)$ and of $(1, 4) \circ (2, 3)$.

35. Find the commutator of $(1, 2, \ldots, i)$ and of $(i, i + 1, \ldots, n)$.

36. The commutator of two permutations is an even permutation.

37. The derived group of $\mathscr{S}_n$ is $\mathscr{A}_n$ (clue: use §7, theorem).

38. What is the centre of $\mathscr{S}_2$?

39. For $n \geqslant 3$, the centre of $\mathscr{S}_n$ reduces to the identical permutation.

40. Consider the subgroup H of $\mathscr{S}_5$ defined by

$$\text{H} = \text{sgr}\,\{(2, 1), (3, 1), (5, 4)\}$$

What is the centre of H?

41. Find a normal subgroup of $\mathscr{A}_4$.

42. For every $n \neq 4$, $\mathscr{A}_n$ is simple.

43. We denote the derived group of G by G'.
And we put $\text{G}'' = (\text{G}')'$, $\text{G}''' = (\text{G}'')'$, etc.
Find S_i', S_i'', S_i''', S_i'''', S_i''''' for $i = 1, 2, 3, 4$ and for $i = n > 4$.

44. CAYLEY's Theorem: Every group of cardinal γ is isomorphic to a subgroup of $\mathscr{S}(\gamma)$.

45. Find a group of permutations isomorphic to Klein's four-group.

46. Find a permutation group isomorphic to the cyclic group of order 71.

47. Find a permutation group isomorphic to the quaternion group.

48. Find a permutation group isomorphic to $\text{Z}_3 \oplus \text{Z}_3$.

9

Groups with Operators

§1. A UNIFYING CONCEPT

The idea of a group with operators—which we shall define later on—generalizes that of a group and increases considerably the range of the theory.

We shall see that vector spaces and ring-modules are groups with operators. The ideals of a ring are substructures of this ring regarded as a group with operators.

Since the fundamental theorems of group theory remain valid in the generalized theory, the idea of a group with operators appears as a unifying concept which is particularly important by virtue of its applications. In particular, it allows us to connect the theory of vector spaces and that of ideals to the same stem of group theory.

After defining and illustrating the concept of a group with operators, we shall see how the fundamental theorems already proved are generalized.

In Chapter X we shall carry straight on with our account within the framework of the theory of groups with operators.

§2. EXAMPLES

(a) Let M, + be a module.

By the properties of the scalar law, in a commutative group every $z \in Z$ defines an endomorphism of M, + which we shall denote by z.

$$z. : \mathrm{M}, + \to \mathrm{M}, + : m \to (z.)(m) = zm$$

We say that Z is a set of operators for M, + and that Z, M, + is a group with operators.

Two distinct operators can define the same endomorphism. Thus, in the case of the module Z_2, + all the even integers define the null endomorphism, and all the odd integers define the identical automorphism.

(b) We know that the set V of vectors of ordinary space having a common origin 0 is a group V, +.

Every homothety of centre 0 defines an endomorphism of V, +. Since the homotheties of centre 0 are completely defined by the radius of similarity, every real number defines an endomorphism of V, +. Thus R is a set of operators for the group V, +. We shall say that V is provided with a scalar multiplication

$$\mathrm{R} \times \mathrm{V} \to \mathrm{V} : (r, v) \to rv \qquad (1)$$

Since $Z \subset R$, the group V is *ipso facto* provided with the set of operators Z. The reader should note that the scalar law $Z \times V \to V$ deduced from (1) by restriction is none other than the scalar law which we defined in Chapter 3 and which we recalled in example (a).

The group with operators R, V, + is called a *vector space*.

(c) Let A, +, . be any ring whatsoever. Every element $a \in A$ defines by left and right multiplication the transformations $a.$ and $.a$ of A:

$$a. : \mathrm{A} \to \mathrm{A} : x \to (a.)(x) = a.x = ax$$
$$.a : \mathrm{A} \to \mathrm{A} : x \to (.a)(x) = x.a = xa$$

Because of the distributivity of the multiplication of a ring with respect to addition, $a.$ and $.a$ are endomorphisms of A, +.

Let us put for the moment

$$\mathrm{A}. = \{a. \mid a \in \mathrm{A}\} \quad \text{and} \quad .\mathrm{A} = \{.a \mid a \in \mathrm{A}\}$$

The commutative group A, + admits the sets A., .A and A. ∪ .A as sets of operators, and consequently

A., A, +
.A, A, +
.A ∪ A., A, +

are groups with operators.

(d) Let G, ∗ be any group whatsoever. We know that every element g of G defines an inner automorphism which we shall denote by $g.$:

$$g. : \mathrm{G}, * \to \mathrm{G}, * : x \to (g.)(x) = g.x = g * x * \bar{g}$$

Every group G, ∗ may therefore be regarded as a group with operators G., G, ∗ where G. is the set of inner automorphisms of G, ∗.

(e) The set auto (G, ∗) of automorphisms of G, ∗ can act as the set of operators for the group G, ∗, giving rise to the group with operators

(auto (G, ∗)), G, ∗

Similarly, the set endo (G, $*$) of endomorphisms of G, $*$ gives rise to the group with operators

$$(\text{endo } (G, *)), G, *$$

§3. GROUPS WITH OPERATORS

Definition. Every set Ω of elements such that every $a \in \Omega$ defines an endomorphism $a.$ of the group G, $*$ *is called a set of operators for* G, $*$.
The structure Ω, G, $*$ *is called a group with operators.*

For every $x \in G$ we shall put $ax = (a.)(x)$.

We may restate the above definition by saying that every group G, $*$ provided with an outer law

$$\Omega \times G \to G : (a, g) \to ag$$

which is distributive with respect to $*$, i.e. such that

$$\forall a \in \Omega; \quad \forall x, y \in G: \qquad a(x * y) = ax * ay$$

is called a group with operators Ω, G, $*$.

If Ω, G, $*$ is a group with operators, we therefore have

$$\forall a \in \Omega, \forall x, y \in G: \qquad a(x * y) = (ax) * (ay)$$
$$a\nu = \nu$$
$$a\bar{x} = \overline{ax}$$

§4. EXERCISES

In some of the exercises below we introduce some fundamental mathematical structures. They are mentioned essentially with the aim of giving the reader some insight into the range of the theory of groups with operators.

1. In the case of a commutative multiplicative group G, . every $z \in Z$ defines by the scalar law an endomorphism of G, . in the form of an exponentiation

$$\forall z \in Z: \qquad G \to G : g \to g^z$$

The formula

$$\forall x, y \in G, \forall z \in Z: \qquad (x.y)^z = x^z.y^z$$

expresses the fact that the transformation $g \to g^z$ is indeed an endomorphism of G, ..

2. In a non-commutative group G, . raising to the power z is again a transformation of G but it is no longer in general an endomorphism of G, ..

(a) Show that in the group of isometries of the plane leaving a point fixed, squaring is not an endomorphism.

To do this it is sufficient to consider the symmetries a and b with respect to distinct straight lines which are not orthogonal and which pass through the fixed point. We then have

$$(b \circ a)^2 \neq b^2 \circ a^2$$

since

$$a^2 = b^2 = I$$

and $(b \circ a)^2$ is a non-identical rotation.

(b) Show that in the group

$$\mathscr{S}\{a, b, c\}$$

squaring is not an endomorphism.

The reader may deduce this from the counter-example

$$I = (c, a)^2 \circ (b, a)^2 \neq ((c, a) \circ (b, a))^2 = (cba)^2 = (abc) = (cba)^{-1} \neq I$$

Enunciate the assertion which appears at the beginning of this exercise in the case of non-commutative groups A, $+$ and B, $*$.

The transformations

$$A \to A : a \to za$$

and

$$B \to B : b \to z \perp b$$

are not in general endomorphisms of A, $+$ and B, $*$.

3. In the module Z_3, $+$ describe the endomorphisms 0., 1. and 2..

4. If Ω, G, $*$ is a group with operators, then $a \to a.$ is a map of Ω into endo (G, $*$).

Determine those groups with operators already encountered for which this map is injective or projective.

5. Let us consider the group Z_n, $+$ provided with the set of operators Z (the endomorphisms being defined by scalar multiplication).

Let $z_1, z_2 \in Z$.

When do we have $z_1. = z_2.$?

Deduce from this a natural way of providing the group Z_n, $+$ with the set of operators Z_n.. What can you say in this last case about the map $(a \to a.)$ of the set of operators into that of endomorphisms?

6. Let G, $*$ be a group. The sets of operators G., auto (G, $*$) and endo (G, $*$) are stable for the product of composition, and we have

$$\mathrm{G}., \circ \subset \mathrm{Auto}\ (\mathrm{G}, *), \circ \subset \mathrm{Endo}\ (\mathrm{G}, *), \circ$$

The outer law

$$(\mathrm{Endo}\ (\mathrm{G}, *)) \times \mathrm{G} \to \mathrm{G}$$

satisfies the law of mixed associativity

$$\forall a, b \in \mathrm{Endo}\ (\mathrm{G}, *), \forall x \in \mathrm{G}: \qquad (a \circ b)(x) = a(b(x))$$

7. Consider a group G, $*$. If f and g are transformations of G, the product $f * g$ defined by

$$\forall x \in \mathrm{G}: \qquad (f * g)(x) = f(x) * g(x)$$

is a new transformation of G, $*$. If f and g are endomorphisms of G, $*$, the same is not necessarily so of $f * g$. To see this it is sufficient to take $f = g = \mathrm{I}$ = the identical automorphism of G. We then have

$$\begin{aligned} \mathrm{I} * \mathrm{I} : \mathrm{G} \to \mathrm{G} : x &\to \mathrm{I}(x) * \mathrm{I}(x) \\ &= x * x \\ &= 2 \perp x \end{aligned}$$

But we know (see Ex. 2) that if G, $*$ is not commutative, the map

$$\mathrm{G} \to \mathrm{G} : x \to 2 \perp x$$

is not in general an endomorphism.

8. For a commutative group G, $*$ the product $f * g$ of two endomorphisms of G, $*$ is a new endomorphism of G, $*$. In other words, Endo (G, $*$) is stable for $*$. We shall establish that the structure

$$(\mathrm{Endo}\ (\mathrm{G}, *)), *$$

is a group. Its neutral element is the neutral endomorphism

$$\mathrm{G} \to \mathrm{G} : g \to \nu$$

which by a new abuse of words we shall often denote by ν.

The symmetric of the endomorphism f in the group under consideration is the endomorphism $\bar{f}$ defined by

$$\bar{f} : \mathrm{G} \to \mathrm{G} : x \to \bar{f}(x) = f(\bar{x})$$

We can therefore write

$$\bar{f}(x) = f(\bar{x}) = \overline{f(x)}$$

In the case of a module M, $+$ the neutral element is the null transformation and the symmetric of the endomorphism t will be denoted by $-t$. The above formula will then be written

$$(-t)(x) = t(-x) = -(t(x))$$

9. The ring of endomorphisms of a module

Let M, $+$ be a module. We know that Endo (M, $+$) is stable for the laws $+$ and $\circ$. We shall establish that the structure

$$(\mathrm{Endo}\ (\mathrm{M}, +)), +, \circ$$

is a ring.

Since the law $\circ$ is associative we simply need to verify the distributive laws

$$\forall f, g, h \in \mathrm{Endo}\ (\mathrm{M}, +): \qquad \begin{aligned} f \circ (g + h) &= f \circ g + f \circ h \\ (f + g) \circ h &= f \circ h + g \circ h \end{aligned}$$

(The first of these rules remains valid in the case of a non-commutative group M, $+$.)

We shall say that

$$(\mathrm{Endo}\ (\mathrm{M}, +)), +, \circ$$

is the ring of operators of M, $+$ and, to simplify our writing, we shall sometimes allow ourselves to omit the $\circ$.

10. Ring modules

The module M, $+$ provided with its ring of operators is a particular example of a ring-module.

For every $x, y \in \mathrm{M}$ and for every $f, g \in \mathrm{Endo\ M}$ we have

$$\begin{aligned} f(x + y) &= f(x) + f(y) \\ (f + g)(x) &= f(x) + g(x) \end{aligned}$$

(The first of these formulae expresses the fact that f is an endomorphism, and the second is none other than the definition of the law $+$ in M^{M}.)†

Definition. We define a ring-module (or more precisely an A*-module) to be a module* W, $+$ *provided with a ring* A, $+, .$ *of operators such that the outer law (or scalar multiplication) is distributive both with respect to addition in* A *and with respect to addition in* W, *and satisfies the rule of mixed associativity.*

If $a \in \mathrm{A}$ and $w \in \mathrm{W}$ it is usual to denote the result of the outer law

† Tr. See revision exercises on Ch. 2, Ex. 13.

by aw. The double distributivity and mixed associativity are then written:

$$\forall a \in A, \forall m, w \in W: \quad a(m + w) = am + aw$$
$$\forall a, b \in A, \forall w \in W: \quad (a + b)w = aw + bw$$
$$\forall a, b \in A, \forall w \in W: \quad a(bw) = (ab)w$$

As a consequence of mixed associativity we can write abw instead of $(ab)w$ or $a(bw)$.

This ring-module will be denoted by A, M, or even simply by M. The elements of A are called the coefficients of the ring-module.

11. We call every ring K, +, . in which $K_0 = K \setminus \{0\}$ is a group for the multiplication of the ring a *skew field*.

The reader should show that in a skew field K

$$\forall a, b \in K: \quad a.b = 0 \Rightarrow a = 0 \quad \text{or} \quad b = 0$$

The structures

Q, +, .; R, +, .; C, +, . are commutative skew fields or fields.

The multiplicative group K_0, . of the skew field K, +, . contains a neutral element which we shall usually denote by 1.

12. Let K, +, . be a skew field.

Every ring-module K, V in which

$$\forall v \in V: \quad 1v = v$$

is called a *vector space* over the skew field K.

The reader should establish that

$$\forall k \in K; \quad \forall v \in V: \quad kv = 0 \Rightarrow k = 0 \quad \text{or} \quad v = 0$$

Note the abuses of notation which have just been made: the first and the third zero denote the neuter of the group V, + while the second zero denotes the neuter of K, +.

13. The group with operators R, V, + (defined in §2, b) is a vector space. This structure explains the terminology used more generally.

14. Let us consider the set R^R of transformations of R (or of functions defined on R with real values). We know that R^R is a group for the addition of functions. For every $r \in R$ and $f \in R^R$, let us define $rf \in R^R$ as usual by putting $\forall x \in R: \quad (rf)(x) = r.f(x)$.

In this way R^R is made into a vector space over the field R.

15. The set of continuous functions with real values defined on the segment [0, 1] is a real vector space, i.e. a vector space over R. (We understand here that the inner and outer laws are defined in the natural way.)

§5. ADMISSIBLE SUBGROUPS

Let Ω, G, ∗ be a group with operators.

Every subgroup S of G, ∗ which is itself a group with operators Ω, S, ∗ will be called admissible. This will be so if and only if S is stable for all the operators of Ω.

Definition. The subgroup S *of* G, ∗ *is an admissible subgroup of* Ω, G, ∗ *if and only if* $\forall a \in \Omega, \forall s \in S: \quad as \in S$.

Exercise

For every subset A of Ω and for every subset B of G, it is natural to put $AB = \{ab \mid a \in A, b \in B\}$.

A subgroup S of G, ∗ is therefore admissible if and only if $\Omega S \subset S$.

Examples

1. The admissible subgroups of G., G, ∗ are none other than the normal subgroups of G, ∗.

2. The admissible subgroups of auto (G, ∗), G, ∗ are the characteristic subgroups of G, ∗.

What are the admissible subgroups of endo (G, ∗), G, ∗?

3. Let A, +, . be a ring. The admissible subgroups of A., A, + are called the *left ideals of the ring* A, +, ..

Define similarly the *right ideals*.

The admissible subgroups of A. ∪ .A, A, + are called the (*bilateral*) *ideals of the ring* A.

4. Z is a subgroup of R, + but it is not an admissible subgroup of R, R, +.

5. Since we have not made any hypothesis about the set of operators Ω, the theory which we develop remains valid if $\Omega = \varnothing$. In this case the admissible subgroups of Ω, G, ∗ are none other than the subgroups of G, ∗.

6. Consider the vector space V formed by the vectors of space having a fixed point 0 as origin. Let v be a non-null vector of V. The subgroup of V, + generated by v is the set $Zv = \{zv \mid z \in Z\}$. This is not an admissible subgroup. It is easy to see that the

smallest admissible subgroup or vector subspace of the vector space V which contains v is the set

$$Rv = \{rv \mid r \in R\}$$

The admissible subgroups of a vector space are called vector subspaces.

§6. THEOREM

Every intersection of admissible subgroups is an admissible subgroup.

Let $\mathscr{S}$ be a set of admissible subgroups of the group with operators $\Omega, G, *$. We already know that the intersection $\cap\mathscr{S}$ of this set of subgroups of $G, *$ is a subgroup of $G, *$.

It remains to prove that $\cap\mathscr{S}$ is an admissible subgroup.

Let $x \in \cap\mathscr{S}$ and $a \in \Omega$. We must establish that $ax \in \cap\mathscr{S}$.

Since $x \in \cap\mathscr{S}$, we have $x \in S$ for every $S \in \mathscr{S}$. Since every $S \in \mathscr{S}$ is an admissible subgroup it follows that $ax \in S$ for every $S \in \mathscr{S}$. Hence $ax \in \cap\mathscr{S}$.

Q.E.D.

Proofs of this kind will be omitted from the subsequent work.

Corollary. Every subset P *of* G *generates an admissible subgroup of* $\Omega, G, *$.

In other words, given a subset P of G, there exists an admissible subgroup of $\Omega, G, *$ which contains P and which is included in every admissible subgroup containing P.

The admissible subgroup generated by P is the intersection of all the admissible subgroups which contain P.

§7. EXERCISES

1. Trivial admissible subgroups.

Every group with operators $\Omega, G, *$ has admissible subgroups $\{v\}$ and G. These are the trivial admissible subgroups of Ω, G.

Similarly $\{0\}$ and A are bilateral ideals of the ring $A, +, .$. These are the trivial ideals of this ring.

2. The only ideals of a skew field are its trivial ideals.

3. Every subgroup of $Z, +$ is an ideal of $Z, +, .$.

4. Every intersection of normal subgroups of a group $G, *$ is a normal subgroup.

Every subset P of a group generates a normal subgroup.

Enunciate and justify analogous propositions for characteristic subgroups and endostable subgroups.

5. Every intersection of ideals of a ring is an ideal.

Every subset of a ring generates an ideal.

Give analogous propositions for left and right ideals.

6. Every intersection of vector subspaces is a vector subspace.

Every subset of a vector space generates a vector subspace.

7. A subset I of a ring A is a left ideal if and only if

$$\forall a \in A; \quad \forall x, y \in I: \qquad x - y \in I \quad \text{and} \quad ax \in I$$

8. A subset S of a vector space V over a skew field K is a vector subspace if and only if

$$\forall a, b \in K \quad \text{and} \quad \forall x, y \in S: \qquad ax + by \in S$$

9. If A is an admissible subgroup and B a normal admissible subgroup of $\Omega, G, *$, the product $A * B = B * A$ is an admissible subgroup of $\Omega, G, *$.

10. If S and T are vector subspaces of the vector space V, the sum $S + T$ is a vector subspace of V.

11. The sum of two ideals of a ring is an ideal.

12. Consider a group with operators $\Omega, G, *$. Let P be a subset of G. If A is the subgroup of $G, *$ generated by P and B is the admissible subgroup of $\Omega, G, *$ generated by P, we must have $A \subset B$.

13. Consider the set $R[x]$ of polynomials with real coefficients in the indeterminate x.

The structure $R[x], +$ is a group.
The structure $R, R[x], +$ is a vector space.
The structure $R[x], +, .$ is a ring.

The polynomial $x^2 + 1$ generates in the group $R[x]$ the subgroup: $\{z(x^2 + 1) \mid z \in Z\}$; in the vector space $R[x]$, the vector subspace: $\{r(x^2 + 1) \mid r \in R\}$; in the ring $R[x]$, the ideal: $\{p(x^2 + 1) \mid p \in R[x]\}$.

14. Let P be a subset of the group with operators $\Omega, G, *$. Describe the elements of the admissible subgroup of G generated by P.

§8. THE QUOTIENT BY AN ADMISSIBLE NORMAL SUBGROUP

Let $\Omega, G, *$ be a group with operators and N an admissible normal subgroup.

We shall show that the quotient group $G/N, *$ can be made naturally into a group with operators $\Omega, G/N, *$.

To do this we define the outer law

$$\Omega \times G/N \to G/N : (a, g * N) \to a(g * N)$$

by putting $a(g * N) = ag * N$.

We must justify this definition of the outer law by showing that it depends only apparently on the choice of the element g representing the class $g * N$. In other words we must prove that the formula

$$g_1 * N = g_2 * N \tag{1}$$

implies

$$a(g_1 * N) = a(g_2 * N) \tag{2}$$

In effect:

$g_1 * N = g_2 * N$
$\Rightarrow \bar{g}_1 * g_2 \in N$
$\Rightarrow a(\bar{g}_1 * g_2) \in N$ (because N is admissible)
$\Rightarrow a\bar{g}_1 * ag_2 \in N$ (because the outer law defines an endomorphism of $G, *$)
$\Rightarrow a(g_1 * N) = a(g_2 * N)$

It is clear that every element of Ω does in fact define an endomorphism of $G/N, *$.

Denote by φ the canonical homomorphism

$$\varphi : G \to G/N : g \to g * N$$

We are going to show that this homomorphism "commutes" with the operators:

$$\forall a \in \Omega, \forall g \in G : \varphi(ag) = a\varphi(g)$$

For:

$\varphi(ag) = ag * N$ (definition of φ)
$= a(g * N)$ (definition of the outer law of $\Omega, G/N$)
$= a\varphi(g)$ (definition of φ)

Definition. Let

$$\Omega, G, * \quad \text{and} \quad \Omega, H, *$$

be groups with operators. An admissible homomorphism of $\Omega, G, *$ *into* $\Omega, H, *$ *is a group homomorphism* $h : G, * \to H, *$ *which commutes with the operators, i.e. such that:*

$$\forall a \in \Omega, \forall x \in G : \quad h(ax) = ah(x)$$

Admissible homomorphisms are sometimes called homomorphisms of groups with operators or Ω-homomorphisms.

Theorem – The canonical map of a group with operators onto its quotient by an admissible normal subgroup is an admissible homomorphism.

Examples and Exercises

1. If V and W are vector spaces over the same skew field K, the admissible homomorphisms are called *linear maps*.

The map $t : V \to W$ is linear if and only if

$$\forall a, b \in K; \quad \forall x, y \in V : \quad t(ax + by) = at(x) + bt(y)$$

2. We know that, with a point of ordinary space called 0, the set of points of the space can be made naturally into a vector space R, V, +. Every straight line D containing the origin then appears as a vector subspace. The quotient V/D is the set of straight lines parallel to D, and is provided with the structure of a real vector space. Study the situation which would arise by substituting a plane P for the line D.

§9. THE IMAGE AND KERNEL OF AN ADMISSIBLE HOMOMORPHISM

Theorem – The image and the kernel of admissible homomorphisms are admissible subgroups.

We know that the image and the kernel are subgroups. It remains to prove that they are admissible.

Let Ω, G and Ω, H be groups with operators and $h : G \to H$ an admissible homomorphism.

To establish the first part of the theorem we must show that:

$$\forall a \in \Omega : \quad y \in hG \Rightarrow ay \in hG$$

Since $y \in hG$, there exists $x \in G$ such that $y = h(x)$, whence $ay = ah(x) = h(ax) \in hG$.
(the second equality arises from the fact that h is admissible).

To establish the second part of the theorem we must prove that

$$\forall a \in \Omega : \quad x \in h^{-1}v \Rightarrow ax \in h^{-1}v$$

or, which is equivalent,

$$\forall a \in \Omega: \qquad hx = \nu \Rightarrow h(ax) = \nu$$

which follows from the following working:

$$\begin{aligned} h(ax) &= a(hx) && (h \text{ is admissible}) \\ &= a\nu \\ &= \nu && (\text{since the operator } a \text{ defines an endomorphism of H, } *) \end{aligned}$$

Q.E.D.

Exercises

1. Let Ω, G and Ω, H be groups with operators and $h : G \to H$ an admissible homomorphism. The image by h of every admissible subgroup of G is an admissible subgroup of H.

2. The inverse image by h of every admissible subgroup of H is an admissible subgroup of G containing the kernel of h.

3. The image of every admissible normal subgroup of G is an admissible normal subgroup of hG.

4. The inverse image of every admissible normal subgroup of H is an admissible normal subgroup of G.

5. We know that the image by a homomorphism of every normal subgroup of a group G, $*$ (without operators) is a normal subgroup of the image hG. We can deduce this result from the general proposition which states that the image of an admissible subgroup by an admissible homomorphism $G \to H$ is an admissible subgroup of H.

To do this let us start by noting that the proposition to be proved is equivalent to establishing that the image of a normal subgroup by an epimorphism is a normal subgroup.

Therefore let

$$h : A, * \to B, *$$

be a group epimorphism.

We shall provide the two groups A, $*$ and B, $*$ with the set of operators A, each operator of A defining an endomorphism of A, $*$ in the first case and an endomorphism of B, $*$ in the second case—in the following natural way:

$$\begin{aligned} &\forall g \in A, \forall a \in A: && ga = g * a * \bar{g} \\ &\forall g \in A, \forall b \in B: && gb = (hg) * b * (h\bar{g}) \end{aligned}$$

It is evident that the set of endomorphisms of A, $*$ thus defined by the operators belonging to A is the set of inner automorphisms of A, $*$.

Moreover, since h is a projection we may claim that the set of endomorphisms of B, $*$ thus defined by the operators belonging to A is the set of inner automorphisms of B, $*$.

Thus the admissible subgroups of A, A, $*$ are the normal subgroups of A, $*$ and the admissible subgroups of A, B, $*$ are the normal subgroups of B, $*$.

Let us show that the given epimorphism h is an admissible epimorphism for the new set of operators.

$$\begin{aligned} \forall g \in A, \forall a \in A: \qquad h(ga) &= h(g * a * \bar{g}) \\ &= h(g) * h(a) * h(\bar{g}) \\ &= h(g) * h(a) * \overline{h(g)} \\ &= gh(a) \end{aligned}$$

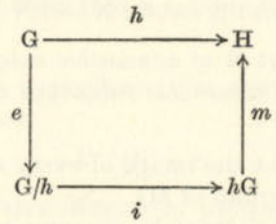
§10. HOMOMORPHISM THEOREM FOR GROUPS WITH OPERATORS

Let

$$h : \Omega, G, * \to \Omega, H, *$$

be a homomorphism of groups with operators.

The homomorphism theorem for groups remains valid, hence the commutative diagram.



(see Ch. 7, §7).

We know that the image hG is an admissible subgroup of Ω, H and that $G/h = G/h^{-1}\nu$ can be made canonically into a group with operators Ω, G/h. Moreover we know that the epimorphism e is admissible and it is obvious that the monomorphism m is admissible.

Let us show that the isomorphism i is admissible.

In fact, with the obvious notations, we have:

$$\begin{aligned} i(a(g * h^{-1}\nu)) &= i(ag * h^{-1}\nu) && (\text{definition of the outer law in } G/h) \\ &= h(ag) && (\text{definition of } i) \\ &= ah(g) && (\text{because } h \text{ is admissible}) \\ &= ai(g * h^{-1}\nu) && (\text{definition of } i) \end{aligned}$$

Q.E.D.

Theorem – Every admissible homomorphism of groups with operators

$$h : \Omega, \mathrm{G}, * \to \Omega, \mathrm{H}, *$$

is the composite

$$h = m \circ i \circ e$$

of the admissible epimorphism

$$e : \Omega, \mathrm{G}, * \to \Omega, \mathrm{G}/h, * : x \to h^{-1}hx$$

the admissible isomorphism

$$i : \Omega, \mathrm{G}/h, * \to \Omega, h\mathrm{G}, * : h^{-1}hx \to hx$$

and the admissible monomorphism

$$m : \Omega, h\mathrm{G}, * \to \Omega, \mathrm{H}, * : y \to y$$

HOMOMORPHISMS AND SUBGROUPS

Theorem – Let

$$h : \Omega, \mathrm{G}, * \to \Omega, \mathrm{H}, *$$

be a homomorphism of groups with operators. The map

$$\check{h} : \mathfrak{R} \to \mathscr{I} : \mathrm{N} \to h\mathrm{N}$$

is a bifunction of the set $\mathfrak{R}$ of admissible subgroups of G *containing* $h^{-1}(\nu)$ *onto the set $\mathscr{I}$ of admissible subgroups of* hG, *in which normal subgroups correspond.*

We already know that the image of every admissible subgroup of G is an admissible subgroup of hG.

The rest of the proof depends on some propositions which are important in themselves, the detailed proofs of which are given below.

Proposition 1. *The inverse image of every admissible subgroup* K *of* H *is an admissible subgroup of* G *containing* $h^{-1}(\nu)$.

Let $x, y \in h^{-1}\mathrm{K}$, $a \in \Omega$. We have:

$$\begin{aligned}
x, y \in h^{-1}\mathrm{K} &\Rightarrow h(x), h(y) \in \mathrm{K} && \text{(definition of } h^{-1}\mathrm{K}) \\
&\Rightarrow h(x) * \overline{h(y)} \in \mathrm{K} && \text{(K is a subgroup)} \\
&\Rightarrow h(x) * h(\bar{y}) \in \mathrm{K} && \text{(the symmetric of the image =} \\
& && \text{the image of the symmetric)} \\
&\Rightarrow h(x * \bar{y}) \in \mathrm{K} && (h \text{ is a homomorphism}) \\
&\Rightarrow x * \bar{y} \in h^{-1}\mathrm{K} && \text{(definition of } h^{-1}\mathrm{K})
\end{aligned}$$

$$\begin{aligned}
a \in \Omega, x \in h^{-1}\mathrm{K} &\Rightarrow a \in \Omega, h(x) \in \mathrm{K} && \text{(definition of } h^{-1}\mathrm{K}) \\
&\Rightarrow a(h(x)) \in \mathrm{K} && \text{(K is admissible)} \\
&\Rightarrow h(ax) \in \mathrm{K} && (h \text{ is admissible}) \\
&\Rightarrow ax \in h^{-1}\mathrm{K} && \text{(definition of } h^{-1}\mathrm{K})
\end{aligned}$$

Q.E.D.

Proposition 2. *For every admissible subgroup* S *of* G *we have*

$$h^{-1}h\mathrm{S} = \mathrm{S} * h^{-1}\nu$$

In fact

$$\begin{aligned}
x \in h^{-1}h\mathrm{S} &\Leftrightarrow h(x) \in h\mathrm{S} \\
&\Leftrightarrow \exists s \in \mathrm{S}: \quad h(x) = h(s) \\
&\Leftrightarrow \exists s \in \mathrm{S}: \quad h(x) * \overline{h(s)} = \nu \\
&\Leftrightarrow \exists s \in \mathrm{S}: \quad h(x) * h(\bar{s}) = \nu \\
&\Leftrightarrow \exists s \in \mathrm{S}: \quad h(x * \bar{s}) = \nu \\
&\Leftrightarrow \exists s \in \mathrm{S}: \quad x * \bar{s} \in h^{-1}\nu
\end{aligned}$$

It follows that

$$\forall x \in h^{-1}h\mathrm{S}: \qquad x = (x * \bar{s}) * s \in h^{-1}(\nu) * \mathrm{S} = \mathrm{S} * h^{-1}(\nu)$$

since $h^{-1}(\nu)$ is normal. Hence $h^{-1}h\mathrm{S} \subset \mathrm{S} * h^{-1}(\nu)$. On the other hand it is immediately clear that $\mathrm{S} * h^{-1}(\nu) \subset h^{-1}h\mathrm{S}$.

Q.E.D.

Proposition 2 has as a corollary: *For every admissible subgroup* S *containing* $h^{-1}(\nu)$ *we have*

$$h^{-1}h\mathrm{S} = \mathrm{S}$$

The map $\check{h}$ is projective because of proposition 1; since for every subgroup K of hG we have:

$$\mathrm{K} = h(h^{-1}\mathrm{K})$$

with $h^{-1}\mathrm{K} \supset h^{-1}(\nu)$.

On the other hand $\check{h}$ is injective; for, let S, T be subgroups of G containing $h^{-1}(\nu)$ such that $\check{h}\mathrm{S} = \check{h}\mathrm{T}$.

We have, by proposition 2:

$$\begin{aligned}
\mathrm{S} &= \mathrm{S} * h^{-1}(\nu) \\
&= h^{-1}h\mathrm{S} \\
&= h^{-1}h\mathrm{T} \\
&= \mathrm{T} * h^{-1}(\nu) \\
&= \mathrm{T}
\end{aligned}$$

The map $\check{h}$ is therefore a bifunction of the set of admissible subgroups of G containing $h^{-1}(\nu)$ onto the set of admissible subgroups of hG.

We prove finally that the restriction of $\check{h}$ to the set of normal admissible subgroups of G containing $h^{-1}(\nu)$ is a bifunction of the set of normal admissible subgroups of G containing $h^{-1}(\nu)$ onto the set of normal admissible subgroups of hG.

This assertion follows immediately by the method of extension of the set of operators indicated in §9, Exercise 5, or immediately from §9, Exercise 3.

§11. ISOMORPHISM THEOREMS

Let B and S be normal admissible subgroups of the group with operators Ω, A, $*$ such that $S \subset B \subset A$. It is evident that S is a normal admissible subgroup of B. We shall show that B/S is a normal admissible subgroup of A/S and that the quotient group with operators (A/S)/(B/S) is isomorphic to A/B by an admissible isomorphism.

By the homomorphism theorem for groups with operators, it is sufficient to exhibit an admissible epimorphism

$$A/S \to A/B$$

whose kernel is precisely B/S.

We have seen (Ch. 7 §11) that the map

$$f : A/S \to A/B : a * S \to a * B$$

is an epimorphism with kernel B/S.

This epimorphism is admissible since

$\forall \lambda \in \Omega, \forall a \in A$:

$$\begin{aligned} f(\lambda(a * S)) &= f(\lambda a * S) && \text{(definition of the outer law in A/S)} \\ &= \lambda a * B && \text{(definition of } f\text{)} \\ &= \lambda(a * B) && \text{(definition of the outer law in A/B)} \\ &= \lambda f(a * S) && \text{(definition of } f\text{)} \end{aligned}$$

Theorem – Let B *and* S *be normal admissible subgroups of the group with operators* A, $*$ *such that* $S \subset B \subset A$. *The quotient* B/S *is then a normal admissible subgroup of* A/S *and we have*

$$\boxed{(A/S)/(B/S) \cong A/B}$$

by the admissible isomorphism $(a * S) * B/S \to a * B$.

We leave to the reader the pleasure of adapting the reasoning of Chapter 7, §12 to establish the second isomorphism theorem for groups with operators.

Theorem – Let A *be an admissible subgroup and* B *a normal admissible subgroup of the group* G, $*$; *the intersection* $A \cap B$ *is then a normal admissible subgroup of* A *while* B *is a normal admissible subgroup of the group* $A * B = B * A$. *We have, moreover*

$$A/(A \cap B) \cong (A * B)/B$$

by the admissible isomorphism $a * (A \cap B) \to a * B$.

Revision exercises on Chapter 9

1. Consider the group Z, +, the set ω of natural numbers and the map

$$\omega \times Z \to Z : (n, z) \to nz$$

Prove that ω, Z, + is a group with operators. What are its admissible subgroups?

2. Every commutative group may be regarded as a Z-module. What are its admissible subgroups?

3. Is the hypothesis "commutative" in the preceding exercise essential? Justify your reply.

4. Let G, + be a commutative group and Endo (G, +), +, . the ring of endomorphisms of G (see Ch. 7, Ex. 106). Prove that the outer law

$$(\text{Endo G}) \times G \to G : (f, g) \to f(g)$$

makes G into a group with operators admitting Endo G as set of operators.

5. Let Ω, G, $*$ be a group with operators. Every element of Ω induces an endomorphism in every admissible subgroup of G.

6. We know that every ring A may be regarded as a set of operators of its additive group A, + (by left multiplication). Give numerous examples of rings to show that two distinct operators can induce the same endomorphism of the group.

7. The set {0, 2, 4, 6} provided with addition modulo 8 and with multiplication modulo 8 is a ring. Find a non-null element in this ring which induces the null endomorphism (by multiplication).

8. All the elements of a "ring of null square" (defined Ch. 6, Ex. 13) induce the same endomorphism by multiplication. Which endomorphism?

9. Consider the additive group Z_3, $+$ as a Z-module (see Exercise 2). Find distinct elements of Z which induce the same endomorphism of Z_3, $+$.

10. Denote by $R^{2\times 2}$, $+$ the additive group of 2×2 matrices with real elements. This group is made into a group with operators, admitting R as set of operators, by the definition:

$$\forall r \in R, \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R^{2\times 2}: \qquad r . \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ra & rb \\ rc & rd \end{pmatrix}$$

11. Let G, $*$ be a group. Let Π be any subset of Endo G (the set of endomorphisms of G, $*$). Prove that

$$\Pi, G, *$$

is a group with operators.

12. Let Ω, G, $*$ be a group with operators. The subgroup of G generated by the union of a set of admissible subgroups of Ω, G is an admissible subgroup.

13. Let Ω, G, $*$ be a group with operators. The union of a chain† of admissible subgroups of a group is an admissible subgroup.

14. Let Ω, G, $*$ be a group with operators. Every subset Π of Ω defines naturally a group with operators Π, G, $*$. Every admissible subgroup of Ω, G, $*$ is an admissible subgroup of Π, G, $*$.

15. Let G, $*$ be a group. Take for Ω the set of inner automorphisms of G. What are the admissible subgroups?

16. Let G, $*$ be a group. Put Ω = the set of automorphisms of G. What are the admissible subgroups?

17. The same question taking for Ω the set of endomorphisms of G.

18. Let G, $*$ be a group. What are the subgroups of G admissible for all sets of operators?

19. Is the centre of a group an admissible subgroup whatever the set of operators? (see Revision exercises on Ch. 7, Ex. 77).

20. Prove that the derived group of a group G, $*$ is an admissible subgroup for every group structure with operators Ω, G, $*$.

† Tr. See Ch. 10, § 1.

21. Let G, $*$ be a group. Prove that every normal subgroup of G can be considered in a natural way as a group with operators admitting G as set of operators.

22. Let M, $+$ be a module (or commutative group); let A, $+$, . be a ring. We can make M into an A-module by providing M with the outer law:

$$A \times M \to M : (a, m) \to 0$$

23. Let M, $+$ be a module; let A, $+$, . be a unitary ring (meaning that A contains an element, written 1, such that for every $a \in A$: $a.1 = 1.a = a$). Prove that the following two conditions are equivalent.

(1) $\forall x \in M$: $1.x = x$
(2) $AM = M$
(where $AM = \{a.m \mid a \in A, m \in M\}$).

24. Let M be a module over the ring A, and B a sub-ring of A. Show that M may be regarded as a B-module.

25. Let M be an A-module. Prove that

$$\forall x \in M: \qquad 0.x = 0$$

(where the first 0 belongs to A and the second to M).

26. Let M be an A-module. Prove that

$$\forall a \in A: \qquad a.0 = 0$$

(where the symbol 0 denotes the zero of M).

27. Let M be an A-module. Prove that

$$\forall a \in A, \forall m \in M: \qquad a.(-m) = (-a).m = -(a.m)$$

28. Every ring may be regarded as a module over itself.

29. Every ring may be regarded as a module over any one of its sub-rings.

30. Make a list of axioms defining a vector space V over a skew field K.

31. Every skew field may be regarded as a vector space over any one of its skew sub-fields (in particular over itself).

32. The group of translations of ordinary space is a vector space over the skew field of reals.

33. The group R, $+$ is a vector space over R.

34. The group C, + is a vector space over R.

35. Let G, + be a commutative group. Prove that G may be regarded as an (Endo G)-module (see Ex. 4).

36. Give examples to show that a group with operators Ω, G, $*$ may be generated by a finite subset of G, without $\varnothing$, G, $*$ being able to be generated by a finite subset.

37. Let R, V, + be the vector space formed by the vectors of space having a fixed point 0 as origin.

The group with operators R, V, + has a generating subset comprising three elements, while the group (without operators) V, + does not possess a finite generating subset.

38. What subgroup of V, + is generated by the non-null vector $v \in V$?

39. What is the admissible subgroup of R, V, + generated by the non-null vector $v \in V$?

40. What subgroup of V, + (without operators) is generated by two distinct non-null vectors of V?

41. What is the admissible subgroup of R, V, + generated by two distinct non-null vectors of V?

42. Enunciate the isomorphism theorems for vector spaces.

43. Let A, +, . and B, +, . be rings. A map $A \to B$ is called a homomorphism if and only if

$$\forall x, y \in A: \quad f(x + y) = f(x) + f(y) \quad \text{and} \quad f(x.y) = f(x).f(y)$$

The image of f is a sub-ring of B. Suppose that f is an epimorphism ($f(A) = B$). The assumption that f is an epimorphism allows us to provide the groups A, + and B, + with the set of operators A by putting

$$\forall a, x \in A \quad \text{and} \quad \forall y \in B: \quad ax = a.x \quad \text{and} \quad ay = f(a).y$$

The epimorphism f is then an admissible epimorphism of the groups with operators

$$A, A, + \to A, B, +$$

Deduce from this that the kernel of f is an ideal of A, +, .

Deduce that if K, +, . is a field, every homomorphism of rings

$$h : K, +, . \to B, +, .$$

is either the null homomorphism or a monomorphism.

10

Dimension

§1. THE VECTOR SPACE OF ORDINARY SPACE

We know that as soon as one of its points is taken as origin, ordinary space becomes a real vector space R, V, +. We propose to express by means of the structure R, V, + the fact that "ordinary space is 3-dimensional".

If v_1 denotes a non-null vector of V, there exists a vector v_2 of V which does not belong to the vector space $V_1 = \text{vct}\,(v_1)$ generated by v_1. Whatever the choice of v_2, there exists a vector v_3 of V which does not belong to the vector subspace $V_2 = \text{vct}\,\{v_1, v_2\}$. We then have $V_3 = \text{vct}\,\{v_1, v_2, v_3\} = V$.

Thus we have constructed a chain of vector spaces

$$\{0\} = V_0 \subset V_1 \subset V_2 \subset V_3 = V \tag{1}$$

Since $V_0 \neq V_1 \neq V_2 \neq V_3$ we call this chain strict. Since it is impossible to insert intermediate vector spaces into this chain without its ceasing to be strict, we say that chain (1) is a maximal strict chain.

We characterize the dimension of ordinary space by saying that all the maximal strict chains of vector subspaces of R, V, + consist of three inclusion signs.

Exercises

1. Denote by R, P, + the vector space formed by the ordinary plane as soon as we denote one of its points by 0.

We shall characterize the dimension of R, P, + by saying that all the maximal strict chains of vector subspaces of R, P, + contain two inclusion signs.

2. Denote by R, W, + the vector space formed naturally by the set $R^{1\times 4}$† of sequences of four real numbers. The laws of this vector space are defined by

† Tr. See Revision exercises on Ch. 9, Ex. 10.

$$(a_1, a_2, a_3, a_4) + (b_1, b_2, b_3, b_4) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4)$$
$$k(a_1, a_2, a_3, a_4) = (ka_1, ka_2, ka_3, ka_4)$$

where a, b, k are real numbers.

We characterize the dimension of R, W, + by saying that all the maximal strict chains of vector subspaces of R, W, + contain four inclusion signs.

3. What is the dimension of the vector space R, R, + ? Justify your reply.

4. Show that the real vector space defined by the set of real polynomials in x of degree at most equal to 5 is of dimension 6.

5. Show that the vector space R, R[x], + defined by the set of all real polynomials in x is not of finite dimension.

§2. NORMAL CHAINS

(a) In the general theory of groups with operators the part which we have just seen played by chains of vector subspaces to define dimension will be filled by finite chains of admissible subgroups each of which is normal in its immediate neighbourhood.

Conforming to normal practice, we shall write these chains as descending chains.

Definition. Every chain

$$G = G_1 \supset G_2 \supset G_3 \supset \ldots \supset G_n \supset G_{n+1} = \{v\}$$

of admissible subgroups of a group with operators Ω, G, $*$ *such that for every* $i \in \{2, \ldots, n\}$ G_i *is a normal subgroup of* G_{i-1}, *is called a normal chain of* G.

Examples of normal chains

1. Every group with operators Ω, G, $*$ admits normal chains:
   $G \supset \{v\}$
   $G \supset G \supset \{v\} \supset \{v\} \supset \{v\}$
   $G \supset G \supset G \supset G \supset G \supset \{v\}$
2. $Z_{24} \supset Z_6 \supset Z_6 \supset Z_6 \supset \{0\}$
   $Z_{24} \supset \{0\}$
   $Z_{24} \supset Z_{24} \supset Z_{24} \supset Z_{12} \supset \{0\} \supset \{0\}$
   $Z_{24} \supset Z_{12} \supset Z_6 \supset Z_2 \supset \{0\}$
   $Z_{24} \supset Z_{12} \supset Z_6 \supset Z_3 \supset \{0\}$
   $Z_{24} \supset Z_{12} \supset Z_4 \supset Z_2 \supset \{0\}$

3. Here are some normal chains in the group with operators (which is a vector space) R, R[x], +; (remember that for every subset P $\subset$ R[x], vct (P) denotes the vector subspace generated by P, i.e. the admissible subgroup of R, R[x], + generated by P):

$R[x] \supset \{0\}$
$R[x] \supset R[x] \supset R[x] \supset R[x] \supset \{0\} \supset \{0\}$
$R[x] \supset \text{vct}\{x, x^2\} \supset \text{vct}\{x, x^2\} \supset \text{vct}\{x^2\} \supset \{0\}$
$R[x] \supset \text{vct}\{x, x^2, x^3\} \supset \text{vct}\{x, x^3\} \supset \text{vct}\{x^3\} \supset \{0\}$
$R[x] \supset \text{vct}\{x, x^2, x^5, x^{13}, x^{23}\} \supset \text{vct}\{x^2, x^5, x^{13}, x^{23}\}$
$\supset \text{vct}\{x^2, x^{13}, x^{23}\} \supset \text{vct}\{x^2, x^{23}\} \supset \text{vct}\{x^2\} \supset \{0\}$

Exercise

In a commutative group with operators Ω, M, + all finite chains of admissible subgroups comprising the trivial admissible subgroups are normal.

In particular, all finite chains of vector subspaces comprising the trivial vector subspaces of a vector space V are normal chains of V.

(b) *Definition. If*

$$G = G_1 \supset G_2 \supset G_3 \supset \ldots \supset G_n \supset G_{n+1} = \{v\}$$

is a normal chain of Ω, G, $*$, *the sequence*

$$G_1/G_2, G_2/G_3, \ldots, G_n/G_{n+1}$$

is called the sequence of quotients of the given normal chain.

Definition. Two sequences of groups with operators (all admitting the same set of operators)

$$A_1, A_2, \ldots, A_m$$

and

$$B_1, B_2, \ldots, B_n$$

are equivalent if and only if they satisfy the following two conditions:

1. $m = n$

2. *there exists a permutation* p *of* $\{1, 2, \ldots, m\} = \{1, 2, \ldots, n\}$ *such that* $\forall i \in \{1, 2, \ldots, m\} = \{1, 2, \ldots, n\}$: $A_i \cong B_{p(i)}$.

Definition. Two normal chains are equivalent if and only if their sequences of quotients are equivalent.

Exercises

1. The following two sequences of groups are equivalent:

$$R, Z_2, Z_{10}, Z_4, Z_2, Z_2, Z_{10}, Z, \{0\}$$
$$Z_2, \{0\}, Z_{10}, Z_2, Z_4, R, Z_2, Z_{10}, Z$$

Write down all the permutations each of which by its existence allows us to affirm the equivalence of these sequences.

2. Establish that the normal chains of the group with operators $\Omega, G, *$

$$G \supset \{0\} \supset \{0\}$$
$$G \supset G \supset \{0\}$$

are equivalent.

3. Establish the equivalence of the normal chains

$$Z_{200} \supset Z_{20} \supset Z_4 \supset \{0\}$$

and

$$Z_{200} \supset Z_{50} \supset Z_5 \supset \{0\}$$

4. Every group with operators admits non-equivalent normal chains.

5. In a group with operators every normal chain equivalent to a strict normal chain is itself strict.

(c) We have been able to characterize the dimension of certain vector spaces by considering maximal strict chains. In the general theory we shall have to consider maximal strict normal chains.

Definition. Every maximal strict normal chain of a group with operators is called a composition chain.

Thus

$$G = G_1 \supset G_2 \supset G_3 \supset \ldots \supset G_n \supset G_{n+1} = \{v\}$$

is a composition chain of $\Omega, G, *$ if and only if the following conditions are satisfied:

1. Each of the G_i is an admissible subgroup of G;
2. $G_1 \neq G_2 \neq G_3 \neq \ldots \neq G_n \neq G_{n+1}$;
3. $\forall i \in \{2, 3, \ldots, n\}$, G_i is a normal subgroup of G_{i-1};
4. $\forall i \in \{2, 3, \ldots, n\}$, the formula $G_{i-1} \supset G' \supset G_i$ where G' is a normal admissible subgroup of G_{i-1} implies $G' = G_{i-1}$ or $G' = G_i$.

Examples of composition chains

1. $Z_{24} \supset Z_{12} \supset Z_6 \supset Z_3 \supset \{0\}$
   $Z_{24} \supset Z_{12} \supset Z_6 \supset Z_2 \supset \{0\}$
   $Z_{24} \supset Z_{12} \supset Z_4 \supset Z_2 \supset \{0\}$
   $Z_{24} \supset Z_8 \supset Z_4 \supset Z_2 \supset \{0\}$

2. Denote by $\mathscr{P}_4$ the vector subspace of R[X] whose elements are the polynomials of degree at most equal to 3.

   $\mathscr{P}_4 \supset \text{vct}\{1, X, X^2\} \supset \text{vct}\{1, X\} \supset \text{vct}\{1\} \supset \{0\}$
   $\mathscr{P}_4 \supset \text{vct}\{1, X^2, X^3\} \supset \text{vct}\{1, X^2\} \supset \text{vct}\{X^2\} \supset \{0\}$
   $\mathscr{P}_4 \supset \text{vct}\{X, X^2, X^3\} \supset \text{vct}\{X, X^3\} \supset \text{vct}\{X^3\} \supset \{0\}$

Examples of normal chains which are NOT *composition chains*

1. $Z_{24} \supset Z_{12} \supset Z_3 \supset \{0\}$
   $Z_{24} \supset Z_{12} \supset Z_{12} \supset Z_6 \supset Z_3 \supset \{0\}$
   $Z_{24} \supset \{0\}$

2. $R[X] \supset \mathscr{P}_4 \supset \text{vct}\{1, X, X^2\} \supset \text{vct}\{1, X\} \supset \text{vct}\{1\} \supset \{0\}$
   $R[X] \supset \{0\}$
   $R[X] \supset \mathscr{P}_4 \supset \text{vct}\{1, X, X^2\} \supset 0$

The importance of the idea of a composition chain appears in the Jordan–Hölder theorem whose proof constitutes the main part of this chapter.

Enunciation of the Jordan (1869)*–Hölder* (1889) *theorem – If a group with operators* $\Omega, G, *$ *admits a composition chain, all its composition chains are equivalent.*

In particular, then, all the chains contain the same number of inclusion signs. Since, in the case of vector spaces of ordinary space and their subspaces this number is none other than the dimension, the Jordan–Hölder theorem provides a generalization of this concept.

Exercises

1. We know that every proper subgroup of Z is of the form nZ with $n \in \omega_0$. For every $k \in \omega_0$ we have

$$nZ \supset (kn)Z$$

Deduce from this that Z, + does not admit a composition chain.

2. We know that

$$\forall m, n \in \omega_0: \qquad Z_n \supset Z_m \Leftrightarrow m|n$$

Using the preceding proposition, determine all the composition chains of the group Z_{120}, $+$.

§3. PROOF OF THE JORDAN–HÖLDER THEOREM

We have ascertained that in R, V, $+$ the composition chains—i.e. the longest strict normal chains—provide us with very precise information. In R, V, $+$ every non-maximal strict normal chain may be refined into a composition chain by inserting new vector subspaces.

Definition. We define a refinement of a normal chain to be any chain obtained from the original chain by the insertion of admissible subgroups (distinct or not from the subgroups of the given chain).

We admit that every normal chain is a refinement of itself.
This definition applies to all normal chains (strict or not).

Exercises

1. The chain

$$Z = 1Z \supset 2Z \supset 18Z \supset 90Z \supset 9{,}000Z \supset 0Z$$

admits amongst others the following refinements:

$Z = 1Z \supset 2Z \supset 6Z \supset 18Z \supset 90Z \supset 450Z \supset 9{,}000Z \supset 0Z$
$Z = 1Z \supset Z \supset 2Z \supset 2Z \supset 18Z \supset 90Z \supset 90Z \supset 9{,}000Z \supset 0Z$
$Z = 1Z \supset 2Z \supset 6Z \supset 6Z \supset 18Z \supset 90Z \supset 9{,}000Z \supset 90{,}000Z \supset 0Z$

2. If the chain A is a refinement of the chain B which is itself a refinement of the chain C, the chain A is a refinement of the chain C.

3. Refine the following chains in R, V, $+$ into composition chains.

$$\begin{array}{lll} V \supset \mathrm{vct}\{v_1, v_2\} \supset \{0\} \\ V \supset \mathrm{vct}\{v_1\} \quad \supset \{0\} \\ V \supset \qquad\qquad\quad \{0\} \end{array}$$

where v_1 and v_2 are vectors such that $v_2 \notin \mathrm{vct}\{v_1\}$.

4. Refine the strict chain

$$V \supset \mathrm{vct}\{v_1, v_2\} \supset \mathrm{vct}\{v_1\} \supset \{0\}$$

of R, V, $+$.

5. What can you say about every refinement of a composition chain of a group with operators?

The fundamental result on the refinement of chains in groups with operators is provided by Schreier's (1928) theorem which we shall prove in the next paragraph.

Enunciation of Schreier's theorem – In every group with operators any two normal chains admit equivalent refinements.

We show that Schreier's theorem implies the Jordan–Hölder theorem.

Suppose that the group $\Omega, G, *$ admits the composition chain

$$G = G_1 \supset G_2 \supset G_3 \supset \ldots \supset G_n \supset G_{n+1} = \{v\} \qquad (1)$$

We must prove—using Schreier's theorem—that every composition chain

$$G = H_1 \supset H_2 \supset H_3 \supset \ldots \supset H_m \supset H_{m+1} = \{v\} \qquad (2)$$

of $\Omega, G, *$ is equivalent to (1).

Proof

By virtue of Schreier's theorem the composition chains (1) and (2) admit equivalent refinements (1′) and (2′) respectively.

Since (1) is a composition chain, (1′) is identical to (1) or is obtained from (1) by inserting groups which already appear in (1); we therefore pass from the sequence of quotients of (1) to the sequence of quotients of (1′) by inserting groups all isomorphic to $\{v\}$.

Similarly for (2) and its refinement (2′).

Since (1) and (2) are composition chains the neutral group does not appear in their sequences of quotients. Therefore the equivalence of (1′) and (2′) implies that of (1) and (2).

Q.E.D.

Definition. A group with operators is said to be of finite dimension if and only if it admits a composition chain. The number of inclusion signs appearing in each of these composition chains is called the dimension of the group.

The Jordan–Hölder and Schreier theorems imply the important

Theorem – In a group with operators of finite dimension every strict normal chain may be refined into a composition chain.

Let C be a composition chain and $\mathscr{N}$ a strict normal chain of the group Ω, G, $*$.

By Schreier's theorem, these chains admit equivalent refinements C′ and $\mathscr{N}'$ respectively.

If C = C′ the theorem is proved, since a normal chain which is equivalent to a composition chain is itself a composition chain.

If C $\neq$ C′ the chain C′ cannot be strict (since C is a maximal strict normal chain). The chain C′ therefore has a certain number of repetitions. Since C′ and $\mathscr{N}'$ are equivalent these chains have the same number of repetitions. The chains C and $\mathscr{N}$ being strict, the repetitions in C′ and $\mathscr{N}'$ arise from the introduction of new subgroups during the refinement. If we suppress in C′ and $\mathscr{N}'$ the groups causing the repetitions we obtain equivalent strict normal chains C″ and $\mathscr{N}''$, refinements of C and $\mathscr{N}$ respectively.

Since C is maximal we have this time C″ = C, and $\mathscr{N}''$ is indeed a composition chain which is a refinement of $\mathscr{N}$.

Q.E.D.

§4. SCHREIER'S THEOREM

Theorem – Two normal chains of a group with operators admit equivalent refinements.

The main lines of the proof of this important theorem go considerably beyond the theory of groups with operators, and are independent of the methods characteristic of group theory.

On the other hand certain details of the proof depend essentially on the theory of groups with operators to the point of requiring the very technical proof of a third isomorphism theorem.

We shall therefore start by describing the main lines of the proof without appealing to the theory of groups with operators. To fix the concepts in our minds we shall give three examples where the details instead of needing the heavy artillery of group theory, are resolved by using very elementary properties of geometry, arithmetic or set theory.

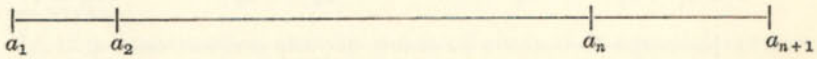
* * *

We must first describe the more abstract ideas independent of group theory which generalize those of a normal chain, a family of quotients and equivalent normal chains.

Normal chains will be generalized by *ladders* which are essentially totally ordered finite sets† (or finite chains) of elements called *steps*. The order relation will be denoted by $\leqslant$.

$$A : a_1 \leqslant a_2 \leqslant \ldots \leqslant a_n \leqslant a_{n+1}$$

can easily be represented by the diagram



In a given normal chain, to every group G_i of the chain there corresponds the quotient

$$G_i/G_{i+1}$$

In a ladder, every step ($\neq a_{n+1}$) will define an object called the *separation* which we shall denote by a_i/a_{i+1}. We shall assume that an equivalence† denoted by $\sim$ is defined for the separations.

Every ladder defines a family of separations; two families of separations $(e_i)_{i\in I}$ and $(u_i)_{i\in I}$ will be called equivalent if and only if there exists a permutation p of I such that

$$\forall i \in I: \qquad e_i \sim u_{p(i)}$$

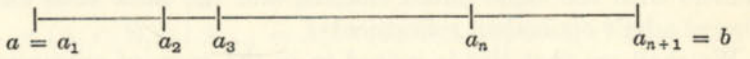
Two ladders having the same initial element and the same final element will be said to be equivalent if and only if their families of separations are equivalent.

* * *

Examples of ladders

1. Every normal chain of a group with operators is a ladder. The steps are the admissible subgroups; the ordering relation is the set-theory inclusion $\supset$. As we said above, the separation G_i/G_{i+1} is none other than the usual quotient of G_i by its normal subgroup G_{i+1}. The separations are therefore also themselves groups and two separations are equivalent if and only if they are isomorphic.

2. Perhaps the most intuitive example of a chain is that furnished by a ladder of points of an ordered segment $[a, b]$.

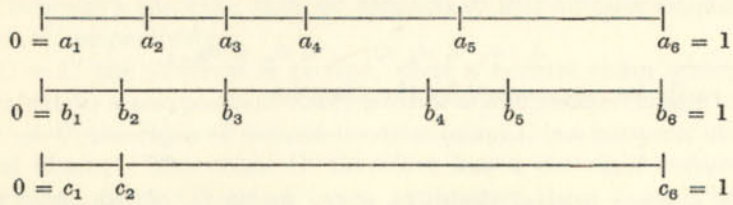


The separation a_i/a_{i+1} of the step a_i is here the distance $(a_i a_{i+1})$.

Two separations will be called equivalent if and only if they are equal.

† Tr. See Appendix.

The first two chains of the diagram below are equivalent. They are not equivalent to the third chain.



3. Let there be given a set E. Every finite chain

$$\mathrm{E} = \mathrm{E}_1 \supset \mathrm{E}_2 \supset \mathrm{E}_3 \supset \ldots \supset \mathrm{E}_n \supset \mathrm{E}_{n+1} = \varnothing$$

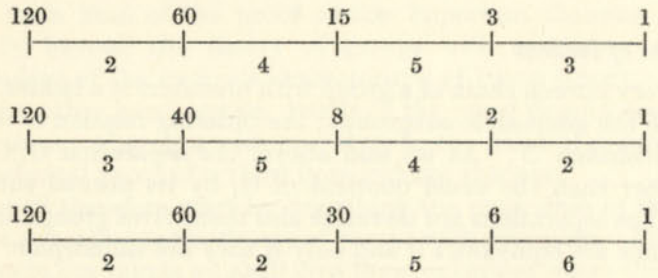
is a ladder with the following definitions.

The separation $\mathrm{E}_i/\mathrm{E}_{i+1}$ is the difference $\mathrm{E}_i \setminus \mathrm{E}_{i+1}$. Two separations are equivalent if and only if they are equal.

4. Every chain of successive divisors of a natural integer ending in 1 is a ladder for the ordering "... is a multiple of ...", with the following definitions.

The separation defined by a divisor is its quotient by the following divisor. Two separations are equivalent if and only if they are equal.

The first two chains of the diagram below are equivalent and they are not equivalent to the third.



The problem which arises implicitly is the following: do two ladders with the same initial element and the same final element always admit equivalent refinements?

We shall see that this is indeed so in the cases of examples 2, 3 and 4 above. The proofs in these cases gradually suggest a method of proof for Schreier's theorem itself.

* * *

Let us consider the two ladders of points of the segment [0, 1].

$$a: \quad 0 = a_1 \leqslant a_2 \leqslant a_3 \leqslant \ldots \leqslant a_m \leqslant a_{m+1} = 1$$
$$b: \quad 0 = b_1 \leqslant b_2 \leqslant b_3 \leqslant \ldots \leqslant b_n \leqslant b_{n+1} = 1$$

We solve the problem by interpolating chain b deprived of its endpoints homothetically† between each successive step of chain a and vice versa.

In this construction the jth point of chain b is mapped between the steps a_i and a_{i+1} of chain a at a point which we denote by $a_{i,j}$.† The steps $b_{j,i}$ are similarly defined.

Clearly we have

$$\forall i = 1, \ldots, m: \qquad a_{i,n+1} = a_{i+1,1} = a_{i+1}$$
$$\forall j = 1, \ldots, n: \qquad b_{j,m+1} = b_{j+1,1} = b_{j+1}$$

The refinement of chain a is therefore formed by the $m.n$ steps $a_{i,j}$ (ordered lexicographically‡ by the double index i, j) and the final step 1.

In the refinement of a, the separation defined by the step $a_{i,j}$ has the value

$$a_{i,j}/a_{i,j+1} = (a_{i+1} - a_i).(b_{j+1} - b_j) \tag{1}$$

As a result of the commutativity of this last product we have

$$a_{i,j}/a_{i,j+1} = b_{j,i}/b_{j,i+1}$$

which establishes the equivalence of the refinements.

* * *

Consider two ladders of subsets of a set E.

$$\mathrm{E} = \mathrm{A}_1 \supset \mathrm{A}_2 \supset \mathrm{A}_3 \supset \ldots \supset \mathrm{A}_m \supset \mathrm{A}_{m+1} = \varnothing$$
$$\mathrm{E} = \mathrm{B}_1 \supset \mathrm{B}_2 \supset \mathrm{B}_3 \supset \ldots \supset \mathrm{B}_n \supset \mathrm{B}_{n+1} = \varnothing$$

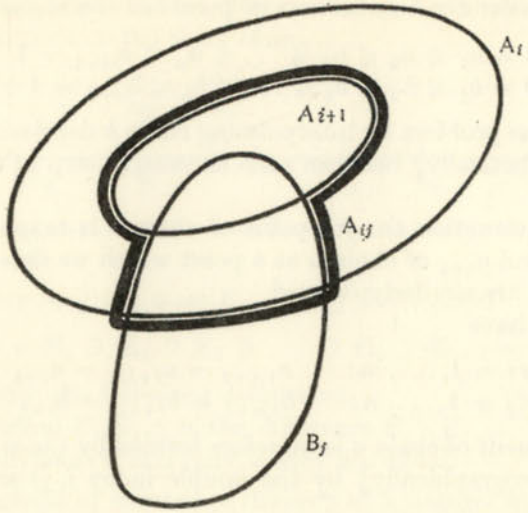
We try to find a construction analogous to that which succeeded so well in the previous example. How can we insert between A_i and A_{i+1} a "reflection" of the chain B? A method quickly springs to mind; map each of the B_j into

$$\mathrm{A}_{i,j} = (\mathrm{A}_i \cap \mathrm{B}_j) \cup \mathrm{A}_{i+1} = \mathrm{A}_i \cap (\mathrm{B}_j \cup \mathrm{A}_{i+1}) = \mathrm{A}_i \cap \mathrm{B}_j \cup \mathrm{A}_{i+1}$$

We define similarly

$$\mathrm{B}_{j,i} = \mathrm{B}_j \cap \mathrm{A}_i \cup \mathrm{B}_{j+1}$$

† Tr. The construction of the points a_{ij} is defined by equation (1).
‡ Tr. See Appendix.



As above, we consider the refined chains formed by the $m.n$ steps $A_{i,j}$, $B_{j,i}$ and the empty set. In the refined chain the separation defined by $A_{i,j}$ is

$$A_{i,j}/A_{i,j+1} = (A_i \cap B_j \cup A_{i+1}) \setminus (A_i \cap B_{j+1} \cup A_{i+1})$$

We shall show that

$$\begin{aligned} A_{i,j}/A_{i,j+1} &= (A_i \cap B_j \cup A_{i+1}) \setminus (A_i \cap B_{j+1} \cup A_{i+1}) \\ &= (B_j \cap A_i \cup B_{j+1}) \setminus (B_j \cap A_{i+1} \cup B_{j+1}) \\ &= B_{j,i}/B_{j,i+1} \end{aligned}$$

This follows immediately from the four-set lemma.

The four-set lemma

$$B \subset A \text{ and } D \subset C \Rightarrow (A \cap C \cup B) \setminus (A \cap D \cup B) = (C \cap A \cup D) \setminus (C \cap B \cup D)\dagger$$

Proof

Consider the difference

$$(A \cap C \cup B) \setminus (A \cap D \cup B) \tag{1}$$

† When we abandon the hypotheses $B \subset A$ and $D \subset C$ we no longer have $(A \cap C) \cup B = A \cap (C \cup B)$, but we can show as an exercise that

$$\begin{aligned} (A \cap C) \cup B \setminus (A \cap D) \cup B &= A \cap (C \cup B) \setminus A \cap (D \cup B) \\ &= C \cap (A \cup D) \setminus C \cap (B \cup D) = (C \cap A) \cup D \setminus (C \cap B) \cup D \end{aligned}$$

By virtue of the formula $(X \cup Z) \setminus (Y \cup Z) = X \setminus (Y \cup Z)$ we will not change the set (1) by suppressing $\cup B$ in the first term of the difference.

By virtue of the formula $(X \cap Y) \setminus (X \cap Z) = (X \cap Y) \setminus Z$ we can then suppress $A \cap$ in the second term of the difference.

Thus

$$\begin{aligned} (A \cap C \cup B) \setminus (A \cap D \cup B) &= (A \cap C) \setminus (D \cup B) \\ &= (C \cap A) \setminus (B \cup D) = (C \cap A \cup D) \setminus (C \cap B \cup D) \end{aligned}$$

Q.E.D.

* * *

Consider the two ladders of successive divisors of the same natural number e.

$$\begin{aligned} e = a_1 \,|^{-1}\, a_2 \,|^{-1}\, a_3 \,|^{-1} \ldots |^{-1}\, a_m \,|^{-1}\, a_{m+1} = 1\dagger \\ e = b_1 \,|^{-1}\, b_2 \,|^{-1}\, b_3 \,|^{-1} \ldots |^{-1}\, b_n \,|^{-1}\, b_{n+1} = 1 \end{aligned}$$

We shall convert this situation into the preceding one by the injection $q : \omega \to \mathscr{P}\omega : x \to q(x)$ where $q(x)$ denotes the set of primary divisors of the natural number x.

Since

$$\forall x, y \in \omega : \quad x|^{-1}\, y \Leftrightarrow q(x) \supset q(y)$$

we have the ladders

$$\begin{aligned} q(e) = q(a_1) \supset \ldots \supset q(a_m) \supset q(1) = \varnothing \\ q(e) = q(b_1) \supset \ldots \supset q(b_n) \supset q(1) = \varnothing \end{aligned}$$

We know that the ladders admit equivalent refinements which we shall obviously denote by

$$q(a_i) \cap q(b_j) \cup q(a_{i+1}), 1 \tag{2}$$

$$q(b_j) \cap q(a_i) \cup q(b_{j+1}), 1 \tag{3}$$

with $i = 1, \ldots, m$; $j = 1, \ldots, n$.

Since

$$\forall x, y \in \omega : \quad q(x \wedge y) = q(x) \cap q(y); \quad q(x \vee y) = q(x) \cup q(y),$$

we have

$$q(a_i) \cap q(b_j) \cup q(a_{i+1}) = q(a_i \wedge b_j \vee a_{i+1}) = q(a_{i,j}) \tag{4}$$

$$q(b_j) \cap q(a_i) \cup q(b_{j+1}) = q(b_j \wedge a_i \vee b_{j+1}) = q(b_{j,i}) \tag{5}$$

† Tr. See Appendix. $x|^{-1}y \Leftrightarrow y|x$, i.e. y divides x.

by putting

$$a_{i,j} = a_i \wedge b_j \vee a_{i+1} \tag{6}$$
$$b_{j,i} = b_j \wedge a_i \vee b_{j+1} \tag{7}$$

And the ladders (ordered lexicographically according to the indices (i, j) and (j, i))

$$a_{i,j},\ 1$$
$$b_{j,i},\ 1$$

(with $i = 1, \ldots, m$; $j = 1, \ldots, n$) are refinements of the ladders of successive divisors of e given initially.

It remains to prove that they are equivalent.

Using formulae (4) and (5) the equivalence of ladders (2) and (3) gives

$$\forall i \in \{1, \ldots, m\};\ \forall j \in \{1, \ldots, n\}: \qquad q(a_{i,j}) \backslash q(a_{i,j+1}) = q(b_{j,i}) \backslash q(b_{j,i+1})$$

It is therefore sufficient to prove that if u and v are natural numbers such that $u|v$, the difference $q(v) \backslash q(u)$ determines v/u.

Denote by $\rho(q(v) \backslash q(u))$ the set of primaries obtained from $q(v) \backslash q(u)$ by dividing every primary $p^n \in q(v) \backslash q(u)$ by p^{m-1}, where p^m is the smallest primary of prime p belonging to $q(v) \backslash q(u)$.

It then follows that

$$\rho(q(v) \backslash q(u)) = q(v/u)$$

which establishes the proposition.

* * *

Consider finally the two normal chains of the group with operators $\Omega, \mathrm{G}, *$

$$\mathrm{G} = \mathrm{G}_1 \supset \mathrm{G}_2 \supset \ldots \supset \mathrm{G}_m \supset \mathrm{G}_{m+1} = \{v\}$$
$$\mathrm{G} = \mathrm{H}_1 \supset \mathrm{H}_2 \supset \ldots \supset \mathrm{H}_n \supset \mathrm{H}_{n+1} = \{v\}$$

The preceding examples suggest the construction of admissible subgroups $\mathrm{grp}\,(\mathrm{G}_i \cap \mathrm{H}_j \cup \mathrm{G}_{i+1})$ generated by the sets $\mathrm{G}_i \cap \mathrm{H}_j \cup \mathrm{G}_{i+1} = (\mathrm{G}_i \cap \mathrm{H}_j) \cup \mathrm{G}_{i+1}$.

The normal subgroup G_{i+1} of G_i commutes with every element of G_i, therefore with every element of $\mathrm{G}_i \cap \mathrm{H}_j$; it follows that the subgroups $(\mathrm{G}_i \cap \mathrm{H}_j)$ and G_{i+1} commute and consequently (see

Revision exercises on Ch. 5, Ex. 1), $(\mathrm{G}_i \cap \mathrm{H}_j) * \mathrm{G}_{i+1}$ is an admissible subgroup of G; whence immediately

$$\mathrm{grp}\,(\mathrm{G}_i \cap \mathrm{H}_j \cup \mathrm{G}_{i+1}) = (\mathrm{G}_i \cap \mathrm{H}_j) * \mathrm{G}_{i+1}$$

In order to emphasize the connection with the preceding example, we start by establishing that

$$(\mathrm{G}_i \cap \mathrm{H}_j) * \mathrm{G}_{i+1} = \mathrm{G}_i \cap (\mathrm{H}_j * \mathrm{G}_{i+1})$$

Proposition 1. *If* A, B, C *are admissible subgroups of* Ω, G, $*$ *such that* B *is a normal subgroup of* A, *the product* $(\mathrm{A} \cap \mathrm{C}) * \mathrm{B}$ *is an admissible subgroup of* Ω, G, $*$ *and we have* $(\mathrm{A} \cap \mathrm{C}) * \mathrm{B} = \mathrm{A} \cap (\mathrm{C} * \mathrm{B})$, *which gives a non-ambiguous meaning to the expression*

$$\mathrm{A} \cap \mathrm{C} * \mathrm{B}$$

It remains to prove only the formula $(\mathrm{A} \cap \mathrm{C}) * \mathrm{B} = \mathrm{A} \cap (\mathrm{C} * \mathrm{B})$.

Let $x \in (\mathrm{A} \cap \mathrm{C}) * \mathrm{B}$. Then $x = u * b$, with $u \in \mathrm{A} \cap \mathrm{C}$ and $b \in \mathrm{B}$. Since $\mathrm{B} \subset \mathrm{A}$, then $b \in \mathrm{A}$; therefore $u \in \mathrm{A}$ and $b \in \mathrm{A}$, whence $x = u * b \in \mathrm{A}$. Since $u \in \mathrm{C}$ and $b \in \mathrm{B}$, we get $x = u * b \in (\mathrm{C} * \mathrm{B})$. Finally $x \in \mathrm{A} \cap (\mathrm{C} * \mathrm{B})$. Therefore $(\mathrm{A} \cap \mathrm{C}) * \mathrm{B} \subset \mathrm{A} \cap (\mathrm{C} * \mathrm{B})$.

Let $x \in \mathrm{A} \cap (\mathrm{C} * \mathrm{B})$. Then $x = c * b$ with $c \in \mathrm{C}$, $b \in \mathrm{B}$ and $c * b \in \mathrm{A}$; since $\mathrm{B} \subset \mathrm{A}$, we have $b \in \mathrm{A}$ and therefore $c \in \mathrm{A}$, hence $c \in \mathrm{A} \cap \mathrm{C}$ and $x = c * b \in (\mathrm{A} \cap \mathrm{C}) * \mathrm{B}$.

Therefore $\mathrm{A} \cap (\mathrm{C} * \mathrm{B}) \subset (\mathrm{A} \cap \mathrm{C}) * \mathrm{B}$.

Q.E.D.

We can therefore quite happily put

$$\boxed{\mathrm{G}_{i,j} = \mathrm{G}_i \cap \mathrm{H}_j * \mathrm{G}_{i+1}}$$

This formula is meaningful for all $i \in \{1, \ldots, m\}, j \in \{1, \ldots, n+1\}$. We note that

$$\mathrm{G}_{i,n+1} = \mathrm{G}_{i+1} = \mathrm{G}_{i+1,1}$$

We define similarly

$$\mathrm{H}_{j,i} = \mathrm{H}_j \cap \mathrm{G}_i * \mathrm{H}_{j+1}$$

which is valid for $j \in \{1, \ldots, n\}$, $i \in \{1, \ldots, m+1\}$.

This time we have $\mathrm{H}_{j,m+1} = \mathrm{H}_{j+1} = \mathrm{H}_{j+1,1}$.

We shall consider the chains of admissible subgroups

$$\mathrm{G}_{i,j}, \{v\} \quad \text{and} \quad \mathrm{H}_{j,i}, \{v\}$$

ordered lexicographically for the double indices.

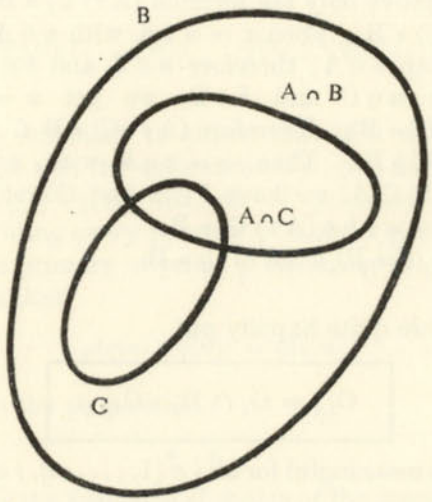
Let us show that $G_{i,j+1}$ is a normal subgroup of $G_{i,j}$.

Since H_{j+1} is a normal subgroup of H_j and G_{i+1} commutes with every element of $G_i \cap H_j$ (and therefore also of $G_i \cap H_{j+1}$) the desired result follows from the following two propositions.

Proposition 2. *If* A, B, C *are admissible subgroups of* Ω, G, $*$ *such that* C *is a normal subgroup of* B, *the intersection* $A \cap C$ *is a normal subgroup of* $A \cap B$.

$A \cap B$ is a subgroup of B, and C is a normal subgroup of B. Therefore the intersection $(A \cap B) \cap C$ (which is none other than $A \cap C$) is a normal subgroup of $A \cap B$.

It follows from this proposition that $G_i \cap H_{j+1}$ is a normal subgroup of $G_i \cap H_j$.



Proposition 3. *If* A, B, C *are admissible subgroups of* Ω, G, $*$ *such that* C *is a normal subgroup of* B, *and if* A *commutes with every element of* B, *the product* $C * A$ *is a normal admissible subgroup of* $B * A$.

Let $a \in A$, $b \in B$.

Since C is a normal subgroup of B we have

$$b * C = C * b \tag{8}$$

Since A commutes with every element of B we have

$$b * A = A * b \tag{9}$$

whence, remembering that $C \subset B$,

$$C * A = A * C \tag{10}$$

We must establish that $C * A$ is normal in $B * A$, i.e. that $C * A$ commutes with every element $b * a$ of $B * A$.

A simple calculation:

$$\begin{aligned}
&b * a * C * A \\
&\quad = b * a * C * A * a && \text{(since } a \text{ is an element of the group A)} \\
&\quad = b * a * A * C * a && \text{(by (10))} \\
&\quad = b * A * C * a && \text{(since } a \text{ is an element of the group A)} \\
&\quad = A * b * C * a && \text{(by (9))} \\
&\quad = A * C * b * a && \text{(by (8))} \\
&\quad = C * A * b * a && \text{(by (10))}
\end{aligned}$$

It follows from proposition 3 that $(G_i \cap H_{j+1}) * G_{i+1}$ is a normal subgroup of $(G_i \cap H_j) * G_{i+1}$.

Before going further let us recapitulate the results already obtained.

Summary – Given the normal chains of the group Ω, G, $*$.

$$\begin{aligned}
G = G_1 \supset G_2 \supset \ldots \supset G_m \supset G_{m+1} = \{\nu\} \\
G = H_1 \supset H_2 \supset \ldots \supset H_n \supset H_{n+1} = \{\nu\}
\end{aligned}$$

we have established that

$$\begin{aligned}
&\forall i = 1, \ldots, m;\ \forall j = 1, \ldots, n+1: && (G_i \cap H_j) * G_{i+1} \\
&&& \quad = G_i \cap (H_j * G_{i+1}) \\
&\forall j = 1, \ldots, n;\ \forall i = 1, \ldots, m+1: && (H_j \cap G_i) * H_{j+1} \\
&&& \quad = H_j \cap (G_i * H_{j+1})
\end{aligned}$$

which allows us to put

$$\begin{aligned}
&\forall i = 1, \ldots, m;\ \forall j = 1, \ldots, n+1: && G_{i,j} = G_i \cap H_j * G_{i+1} \\
&\forall j = 1, \ldots, n;\ \forall i = 1, \ldots, m+1: && H_{j,i} = H_j \cap G_i * H_{j+1}
\end{aligned}$$

We have

$$\begin{aligned}
&\forall i = 1, \ldots, m: && G_{i,n+1} = G_{i+1} = G_{i+1,1} \\
&\forall j = 1, \ldots, n: && H_{j,m+1} = H_{j+1} = H_{j+1,1}
\end{aligned}$$

Let us order the $G_{i,j}$ *(for* $i = 1, \ldots, m;\ j = 1, \ldots, n$) lexicographically for *the double index ij and add to this sequence the neutral group* $\{\nu\}$ *as the* $(mn+1)$*-th element. In this way we obtain a normal refinement of the normal chain* (G_i) *which we shall denote briefly by* $(G_{ij}, \{\nu\})$.

Similarly $(H_{ji}, \{v\})$ *is a normal refinement of the normal chain* (H_j).

In the chain $(G_{ij}, \{v\})$ *the successor of*

$$G_{i,j}(i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\})$$

is $G_{i,j+1}$. *Similarly the successor of* $H_{j,i}(j \in \{1, \ldots, n\}, i \in \{1, \ldots, m\})$ *in the chain* $(H_{ji}, \{v\})$ *is* $H_{j,i+1}$.

It remains to prove that the chains $(G_{ij}, \{v\})$ and $(H_{ji}, \{v\})$ are equivalent.

Taking into account the definition of equivalent normal chains and of the results summarized above, it is sufficient to prove that

$$\forall i \in \{1, \ldots, m\},\ \forall j \in \{1, \ldots, n\}:$$
$$(G_i \cap H_j * G_{i+1})/(G_i \cap H_{j+1} * G_{i+1}) \cong (H_j \cap G_i * H_{j+1})/(H_j \cap G_{i+1} * H_{j+1})$$

This follows from Zassenhaus' theorem
(Vierergruppensatz, or third isomorphism theorem).

The four groups theorem (*Zassenhaus* 1934) – *Let* A, B, C, D *be admissible subgroups of the group with operators* Ω, G, $*$ *such that* B *is a normal subgroup of* A *and* D *a normal subgroup of* C.

$A \cap D * B$ *is then a normal subgroup of* $A \cap C * B$, $C \cap B * D$ *is a normal subgroup of* $C \cap A * D$, *and the quotients are isomorphic.*

$$(A \cap C * B)/(A \cap D * B) \cong (C \cap A * D)/(C \cap B * D)$$

As we mentioned above, the first two assertions of the theorem follow from propositions 2 and 3. It remains to prove the isomorphism.

We shall base this proof on that of the four-set theorem.

There we used two formulae of set-theory

$$(X \cup Z) \setminus (Y \cup Z) = X \setminus (Y \cup Z)$$
$$(X \cap Y) \setminus (X \cap Z) = (X \cap Y) \setminus Z$$

It will suffice to establish analogous formulae for groups.

To do this, we start by observing that the quotient of an admissible subgroup S of Ω, G, $*$ by a normal admissible subgroup N of S is entirely defined by the equivalence (congruence modulo N) provided by the formulae

$$\forall x, y \in S: \qquad x \equiv y \Leftrightarrow x * \bar{y} \in N$$

The same equivalence is defined by a formula

$$\forall x, y \in S: \qquad x \equiv y \Leftrightarrow x * \bar{y} \in P$$

where P is a subset of G.

It will therefore be convenient to denote this quotient also by S/P.

Proposition 4. *If* X, Y, Z *are admissible subgroups of* Ω, G, $*$ *such that* $X * Z$ *and* $(X * Z)/(Y * Z)$ *are groups, we have*

$$(X * Z)/(Y * Z) \cong X/(Y * Z)$$

For every $x \in X$, $z \in Z$ we have $\bar{x} * (x * z) \in Y * Z$ which proves that the element $x * z$ belongs to the class of x.

Q.E.D.

Proposition 5. *If* X *and* Y *are admissible subgroups of* Ω, G, $*$ *and* Z *a subset of* G *such that* $(X \cap Y)/(X \cap Z)$ *is a group, we have*

$$(X \cap Y)/(X \cap Z) \cong (X \cap Y)/Z$$

In fact

$$\forall u, v \in X \cap Y: \qquad \bar{u} * v \in X \cap Z \Leftrightarrow \bar{u} * v \in Z$$

Q.E.D.

Let us apply proposition 4 to the group $(A \cap C * B)/(A \cap D * B)$. We get

$$[(A \cap C) * B]/[(A \cap D) * B] = (A \cap C)/[(A \cap D) * B]$$

Then apply proposition 5 to the group $(A \cap C)/[(A \cap D * B)]$. We get

$$(A \cap C)/[A \cap (D * B)] = (A \cap C)/(D * B) \tag{11}$$

whence $[(A \cap C) * B]/[(A \cap D) * B] = (A \cap C)/(D * B)$.

It remains to permute D and B.

To this effect note that

$$(A \cap C)/(D * B) = (A \cap C)/[(D * B) \cap (A \cap C)]$$

Let us show that

$$(D * B) \cap (A \cap C) = (B * D) \cap (A \cap C) \tag{12}$$

By the symmetry of the formula, it is sufficient to prove

$$(D * B) \cap (A \cap C) \subset (B * D) \cap (A \cap C)$$

Let $x \in (D * B) \cap (A \cap C)$. Then $x = d * b$ with $d \in D$, $b \in B$. But on the other hand $x \in A$, therefore $d * b \in A$. Since $B \subset A$, we get

$b \in A$, hence $d \in A$. Since B is normal in A, there exists $b' \in B$ such that $x = d * b = b' * d$, hence $x \in B * D$ and finally

$$x \in (B * D) \cap (A \cap C)$$

Q.E.D.

We therefore have successively

$$\begin{aligned}
&(A \cap C * B)/(A \cap D * B) \\
&\quad \cong (A \cap C)/(D * B) \\
&\quad \cong (A \cap C)/[(D * B) \cap (A \cap C)] && \text{(by prop. 5)} \\
&\quad \cong (A \cap C)/[(B * D) \cap (A \cap C)] && \text{(by formula (12))} \\
&\quad \cong (C \cap A)/(B * D) && \text{(by prop. 5)} \\
&\quad \cong (C \cap A * D)/(C \cap B * D) && \text{(by (11))}
\end{aligned}$$

This establishes Zassenhaus' theorem, and hence Schreier's theorem.

We have met groups with operators which are not of finite dimension, for example the group Z, +. We propose to see when a group with operators is of finite dimension.

We know (§3) that if $\Omega, G, *$ is of finite dimension every strict normal chain can be refined into a composition chain.

Let H be an admissible subgroup of $\Omega, G, *$ appearing in a normal chain of $\Omega, G, *$. If this group H admitted an infinite ascending sequence of normal admissible subgroups in H, we could construct strict normal chains of $\Omega, G, *$ as long as we liked; and $\Omega, G, *$ would not be of finite dimension.

If a group $\Omega, G, *$ is of finite dimension, the following condition is therefore satisfied:

Emmy Noether's condition (1882–1935): not one of the admissible subgroups of $\Omega, G, *$ in a normal chain of $\Omega, G, *$ admits an infinite ascending chain of normal admissible subgroups. In other words:

If H is a subgroup appearing in a normal chain of $\Omega, G, *$ and if $H_1 \subset H_2 \subset \ldots$ is an ascending chain of normal admissible subgroups of H, there exists $n \in \omega_0$ such that $H_n = H_{n+1} = H_{n+2} = \ldots$.

It is also obvious that the group $\Omega, G, *$ of finite dimension cannot admit an infinite descending chain

$$G = G_1 \supset G_2 \supset \ldots$$

where each of the G_{i+1} is normal in G_i.

Thus every finite-dimensional group satisfies

Emil Artin's condition

If

$$G_1 \supset G_2 \supset \ldots$$

is a descending chain of admissible subgroups of G_1, if G_1 is a normal subgroup of G and if for every $i \in \omega_0$, G_{i+1} is a normal subgroup of G_i, then there exists $n \in \omega_0$ such that $G_n = G_{n+1} = G_{n+2} = \ldots$.

Conversely we shall show that: every group $\Omega, G, *$ simultaneously satisfying the conditions of Noether and of Artin is of finite dimension.

In fact, from Noether's condition, the group G admits (at least) one maximal normal subgroup G_1 (if the normal subgroup N of G is not maximal, there exists a normal subgroup N_1 strictly contained between N and G; if N_1 is not maximal normal, there exists N_2, etc.... Hence an infinite ascending chain of normal subgroups, which is forbidden by Noether's condition). If $G_1 \neq \{v\}$, this same reasoning remains applicable to it: let G_2 be a maximal normal admissible subgroup of G_1. We have thus constructed a chain

$$\begin{array}{ccccccc} G & \supset & G_1 & \supset & G_2 & \supset & \ldots \\ & & \neq & & \neq & & \end{array}$$

As a consequence of Artin's condition, there exists n such that $G_n = \{v\}$. The chain thus constructed is a composition chain.

Theorem – A group is finite-dimensional if and only if it satisfies simultaneously Noether's condition and Artin's condition.

Revision exercises on Chapter 10

1. Let V be the real vector space obtained from ordinary space by denoting one of its points by 0.

We know that we can find in V three vectors e_1, e_2, e_3 such that every $x \in V$ can be expressed uniquely as a linear combination of the e_1, e_2, e_3,

$$x \in V; \quad x = x^1 e_1 + x^2 e_2 + x^3 e_3; \quad (x^1, x^2, x^3 \in R)$$

The base (e_1, e_2, e_3) defines the chain

$$V = V_1 = \text{vct}\{e_1, e_2, e_3\} \supset V_2 = \text{vct}\{e_2, e_3\} \supset V_3 = \text{vct}\{e_3\} \supset \{0\}$$

This chain is a composition chain of the group with operators R, V, +.

We deduce from this that all the bases of V comprise three elements.

2. Generalization of Exercise 1.

If the vector space V over the skew field K admits a finite base $e_1, \ldots, e_n$, all the bases of V consist of n elements. (We say that $\dim V = n$.)

The reader should show that every base defines a composition chain consisting of n inclusion signs.

3. Let A and B be two normal admissible subgroups of Ω, G, $*$. The chains

$$G \supset A \supset \{v\}, \qquad G \supset B \supset \{v\}$$

are normal.

The Schreier equivalent refinements are the chains

$$G \supset B * A \supset A \supset A \cap B \supset \{v\}$$
$$G \supset A * B \supset B \supset A \cap B \supset \{v\}$$

Verify the equivalence of these chains.

4. Schreier's method is coarse and blind. It does not take into account the particular circumstances of the given chains. In the vector space of ordinary space, let P be a vector subspace of dimension 2 and D a vector subspace of dimension 1.

The chains

$$V \supset P \supset \{0\} \quad \text{and} \quad V \supset D \supset \{0\}$$

are equivalent.

The Schreier method blindly provides the equivalent chains

$$V \supset P + D \supset P \supset P \cap D \supset \{0\}$$
$$V \supset P + D \supset D \supset P \cap D \supset \{0\}$$

5. If H is a normal admissible subgroup of the group with operators Ω, G, $*$ there exists a normal chain of G including H.

6. Show that a chain extracted from a normal chain is not necessarily a normal chain.

7. Construct normal chains of the cyclic groups

$$Z, +;\ Z_2, +;\ Z_3, +;\ Z_4, +;\ Z_{24}, +;\ Z_{60}, +$$

8. Construct normal chains
   (a) of Klein's four-group,
   (b) of the symmetric group of degree 3,
   (c) of the quaternion group,
   (d) of the symmetric group of degree 4.

9. Prove that Zassenhaus' theorem implies the second isomorphism theorem.

10. Construct equivalent refinements of the normal chains

$$Z_{960} \supset Z_{240} \supset Z_{12} \supset Z_2 \supset \{0\}$$
$$Z_{960} \supset Z_3 \supset \{0\}$$

of Z_{960}.

11. Find composition chains of the cyclic groups

$$Z_2, +;\ Z_3, +;\ Z_{24}, +;\ Z_{601}, +$$

12. Find composition chains of the groups of order 4 (the cyclic group and Klein's four-group).

13. Can two non-isomorphic groups admit equivalent sequences of quotients? (See Ex. 12.)

14. Find composition chains of the cyclic group of order 6 and of the symmetric group of order 3. Compare the sequences of quotient-groups.

15. Find a composition chain of $\mathscr{S}_n$ for $n \neq 4$.

16. Find a composition chain of $\mathscr{S}_4$.

17. Find composition chains of Z_{120}, $+$ and $\mathscr{S}_5$, $\circ$. Compare the two sequences of quotient-groups.

18. A cyclic group of order 2^n admits only one composition chain.

19. Generalize the preceding proposition.

20. What does the Jordan-Hölder theorem tell us about a group of order $p_1 . p_2$ where p_1 and p_2 are prime numbers?

21. Find two composition chains of R, $R^{2\times 2}$, $+$ (the real vector space of 2×2 real matrices).

What is the dimension of this vector space?

Do you know any other real vector spaces of dimension 4?

22. Let Ω, G, $*$ be a group with operators. A normal admissible subgroup N of G is a maximal normal admissible subgroup of G if and only if G/N is simple.

23. A strict normal chain of a group with operators Ω, G, $*$ is a composition chain of this group if and only if all the groups of its sequence of quotients are simple.

24. Every finite group with operators admits a composition chain.

25. An infinite commutative group without operators does not admit a composition chain.

26. Give counter-examples to show that the hypothesis "without operators" is indispensable (in Ex. 25).

27. Isomorphic groups with operators have the same dimension.

28. A group with operators which admits a composition chain can contain a subgroup which does not admit a composition chain.

Example.† Denote by $\mathscr{S}^{\check{}}(\omega_0)$ the subgroup of $\mathscr{S}(\omega_0)$ whose elements are the permutations of ω_0 which are the product of a finite number of transpositions; denote by $\mathscr{A}^{\check{}}(\omega_0)$ the subgroup of $\mathscr{S}^{\check{}}(\omega_0)$ whose elements are the product of an even number of transpositions.

$\mathscr{A}^{\check{}}(\omega_0)$, $\circ$ admits as a (unique) composition chain:

$$\mathscr{A}^{\check{}}(\omega_0) \supset \{\mathrm{I}\}$$

where I denotes the identical permutation of ω_0.

Show that $\mathscr{A}^{\check{}}(\omega_0)$ contains a subgroup which does not admit a composition chain.

In fact, the subgroup of $\mathscr{A}^{\check{}}(\omega_0)$

$$\mathrm{sgp}\,\{(4n-3, 4n-2)\circ(4n-1, 4n)\,\}\, n \in \omega_0\}$$

is (1) infinite

(2) commutative, since any two elements of the given generating subset commute. The assertion then follows from Exercise 25.

The reader will see that in a finite-dimensional vector space all the vector subspaces are finite-dimensional.

29. The group Q, + is not finite-dimensional because

$$\mathrm{grp}\,(1) \subset \mathrm{grp}\left(\frac{1}{2!}\right) \subset \mathrm{grp}\left(\frac{1}{3!}\right) \subset \ldots \subset \mathrm{grp}\left(\frac{1}{n!}\right) \subset \ldots$$

is an infinite strict chain of subgroups.

30. Enunciate the conditions of Noether and Artin in the case of a commutative group.

† Kurosh, A. G., *The Theory of Groups.*

31. Let N be a normal admissible subgroup of the finite-dimensional group with operators Ω, G, $*$.

Prove that

$$\dim \mathrm{G/N} = \dim \mathrm{G} - \dim \mathrm{N}$$

32. Apply the preceding exercise to vector spaces.

33. Let A be an admissible subgroup and B a normal admissible subgroup of a group with operators Ω, G, $*$. Prove that

$$\dim \mathrm{A} + \dim \mathrm{B} = \dim (\mathrm{A} + \mathrm{B}) + \dim (\mathrm{A} \cap \mathrm{B})$$

34. Apply the preceding exercise to vector spaces.

35. Verify the preceding exercise when G is the vector space of ordinary space and A, B are vector subspaces of dimension 2 (dimension 1 respectively).

36. What is the dimension of a simple group?

Revision exercises on the book

1. Denote by L_n the set of rationals which can be written as terminating decimals in the number system of base n.† Denote by K_n, + the additive group of these numbers modulo 1.

(a) In this group, the chain

$$\{0\} \subset \mathrm{sgp}\,(\cdot 1) \subset \mathrm{sgp}\,(\cdot 01) \subset \mathrm{sgp}\,(\cdot 001) \subset \ldots \subset \mathrm{sgp}\,(\cdot 00\ldots001) \subset \ldots$$

is an infinite strict chain.

(b) Find other infinite strict chains of subgroups of K_n, +.

(c) Is the group K_n, + finite-dimensional?

(d) Show that K_n is the union of the chain shown in (a).

(e) Show that the multiplicative group of n^kth roots of 1, with $k \in \omega_0$, is isomorphic to K_n, +.

(f) Let p be a prime number. For every $k \in \omega_0$: K_p, + admits one and only one cyclic subgroup of order p^k.

(g) Give an infinite proper subgroup of the additive group of terminating decimals modulo 1: K_{10}, +.

(h) Every *proper* subgroup of K_p, + is a *finite* cyclic subgroup whose order is a power of p.

† Tr. See Ch. 4, §14, Ex. 6.

Clue: let S be a proper subgroup of K_p, $+$; there exists therefore an $n \in \omega_0$ such that

$$\cdot 1 \in S;\ \cdot 01 \in S; \ldots; \underbrace{\cdot 00 \ldots 001}_{n-1} \in S;\ \underbrace{\cdot 00 \ldots 001}_{n} \notin S$$

Prove that $S = \text{sgp}\,(\underbrace{\cdot 00 \ldots 001}_{n-1})$

In the theory of commutative groups we prove that the groups K_p, $+$ are the only infinite *commutative* groups all of whose proper subgroups are finite.

(i) The quotient of K_p, $+$ by every proper subgroup is isomorphic to K_p, $+$.

2. What is the subgroup of R, $+$ generated by a pair $\{a, b\}$ of elements of R? (Discuss the different possible cases.)

3. Let A, $*$ and B, $*$ be groups. Is the group G, $*$ determined when we know that $G/A \cong B$? (Clue: $Z_4/Z_2 \cong ?$; $V/Z_2 \cong ?$, where V denotes Klein's four-group.)

4. Let M be a set provided with a law $*$ everywhere defined and associative, admitting a neutral element $\nu \in M$.

Definition: we say that $m \in M$ is *symmetrizable* if and only if there exists $m' \in M$ such that

$$m * m' = m' * m = \nu$$

Prove that the set of symmetrizable elements of M is a group.

5. Let E be a *finite* set provided with a law $*$ which is

(a) everywhere defined.

(b) associative.

(c) $\forall a, b, x \in E$: $(a * x = b * x) \Rightarrow (a = b)$ (right cancellation)
$\forall a, b, x \in E$: $(x * a = x * b) \Rightarrow (a = b)$ (left cancellation).

Prove that E, $*$ is a group.

6. Every finite non-empty stable subset of a group is a subgroup.

7. Let A, B be distinct maximal normal subgroups of a group G, $*$. We have

$$G/A \cong B/(A \cap B)$$

and

$$G/B \cong A/(A \cap B)$$

8. The intersection of two maximal normal subgroups of a group is a maximal normal subgroup of each of them. (See Ex. 7.)

9. Enunciate the Noether and Artin conditions in the case of a commutative group.

10. Write down a composition chain of the vector space R, R, $+$.

11. Let K, $+$, . be a skew field. Write down a composition chain of the vector space K, K, $+$.

12. Every subset of a group isomorphic to a subgroup is itself a subgroup.

13. If a group contains a single subgroup of order $n \in \omega_0$, this subgroup is characteristic.

14. Let us provide $R \times R$ with the law $*$ defined by

$$\forall (a, b), (c, d) \in R \times R: \quad (a, b) * (c, d) = (ad - bc, ac + d)$$

Is this law associative? commutative? Prove that $(0, -1)$ is a left neuter for the law $*$.

Show that $(0, -1)$ is not a right neuter.

Does $R \times R$ admit a neutral element for the law $*$?

What are the elements of $R \times R$ which admit a left symmetric with respect to the left neuter $(0, -1)$?

15. Let H, K be subgroups of the group G, $*$. We have:

$$\forall g_1, g_2 \in G: \quad (H * g_1 * K) \cap (H * g_2 * K) \neq \varnothing \Rightarrow H * g_1 * K = H * g_2 * K$$

16. Let us denote by R[X], $+$ the group of polynomials in the letter X with real coefficients. Which polynomial is the neutral element of the group R[X], $+$? What is the symmetric of $5X^{100} - 3X^2 + \sqrt{2}$?

17. What is the subgroup of R[X], $+$ generated by the following subsets:

(a) $\{5X + 2, X^2, 5\}$.

(b) $\{1\}$.

(c) $\{1, X, X^2, X^3, X^4\}$.

(d) $\{X\}$.

(e) $\{X, X^3, X^5, X^7, X^9, X^{11}\}$.

(f) $\{\frac{1}{2}\}$.

18. What is the vector subspace of R, R[X], + generated by the subsets considered in the preceding exercise?

19. Prove that the subgroups

$$\text{sgp}\,\{X, X^3, X^5, X^7, X^9\} \quad \text{and} \quad \text{sgp}\,\{1, X^2, X^4, X^6, X^8\}$$

of R[X], + are isomorphic.

20. What are the elements of the quotient of R[X], + by sgp $\{1\}$?

21. What are the elements of the quotient of R[X], + by sgp $\{X, X^2, X^7\}$?

22. Find generating subsets of the group Z[X], +.

23. Find generating subsets of the group R[X], +.

24. Denote by $\mathscr{P}_n$ the set of polynomials in X with real coefficients and of degree strictly less than n. Find minimal generating subsets of the vector space R, $\mathscr{P}_n$, +.

25. Construct normal chains of the group R[X], +.

26. Does the group R[X], + satisfy Noether's condition? Artin's condition?

27. Calculate in the group C_0, .:

$$(5 - 2i)^{-1}, i^{-1}, (3 + 4i)^{-1}$$

28. Decompose into disjoint cycles:

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 1 & 2 & 7 & 5 & 11 & 9 & 8 & 10 & 6 & 3 & 4 & 13 & 12 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}^{-5}$

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}^{4}$

29. Find a composition chain of $\mathscr{S}_8$.

30. Find a composition chain of $\mathscr{A}_8$.

31. In the group R/Z, + every rational generates a finite group. Is the same true of $\sqrt{2} + Z$?

32. The skew field of quaternions $\mathscr{Q}$, +, .

$$\mathscr{Q} = \{a + bi + cj + dk \mid a, b, c, d \in R\}$$

We define the laws + and . as follows:

$$(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k)$$
$$= (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k$$

$$(a_1 + b_1 i + c_1 j + d_1 k).(a_2 + b_2 i + c_2 j + d_2 k)$$
$$= a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2 + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)i$$
$$+ (a_1 c_2 + c_1 a_2 + d_1 b_2 - b_1 d_2)j + (a_1 d_2 + d_1 a_2 + b_1 c_2 - c_1 b_2)k$$

Prove that $\mathscr{Q}$, +, . is a skew field.

33. Find the inverse of the following quaternions:

$$i, j, k$$

34. Calculate

$$ij, -ji, jk, -kj, ki, -ik, i^2, j^2, k^2$$

35. Calculate

$$(3 + 4i - 5j + k)^{-1}, (5j - 3k)^{-1}$$

(bear in mind the calculation of the inverse of a complex number).

36. Prove that the polynomial

$$X^2 + 1$$

admits an infinity of quaternions as roots.†

37. Find an isomorphism of the group $\mathscr{Q}$, + onto the additive group of polynomials in X with real coefficients of degree $\leqslant 3$.

38. What is the order of the alternating group of degree 6?

39. Prove that every element of order 21 of $\mathscr{S}_{12}$ is an even permutation. Give examples of such elements.

40. What is the order of the additive group of polynomials in X with coefficients in Z_2 and of degree $\leqslant n$?

41. What is the order of the additive group of polynomials in X with coefficients in Z_m and of degree $\leqslant n$?

42. Prove that

$$R^{1\times n} = \{(x_1, x_2, \ldots, x_n) \mid x_1, x_2, \ldots, x_n \in R\}$$

† Eilenberg and Niven have proved that every polynomial with quaternion coefficients admits a quaternion root (1944).

is made into a vector space over the reals by the following definitions:

(a) $\forall (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in \mathrm{R}^{1\times n}$:
$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n)$
$= (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$

(b) $\forall r \in \mathrm{R}, \forall (x_1, x_2, \ldots, x_n) \in \mathrm{R}^{1\times n}$:
$r(x_1, x_2, \ldots, x_n) = (rx_1, rx_2, \ldots, rx_n)$

43. Find subspaces of $\mathrm{R}, \mathrm{R}^{1\times n}, +$.

44. Generalize Exercises 42 and 43 in the case of any skew field $\mathrm{K}, +, .$ whatsoever.

45. Which of the following subsets of $\mathrm{R}^{1\times n}$ are vector subspaces of $\mathrm{R}, \mathrm{R}^{1\times n}, +$:

(a) $\{(x_1, x_2, \ldots, x_n) \mid x_1 = 0\}$;
(b) $\{(x_1, x_2, \ldots, x_n) \mid x_1 = 0 \text{ and } x_2 = 0\}$;
(c) $\{(x_1, x_2, \ldots, x_n) \mid x_1 = 0 \text{ or } x_2 = 0\}$;
(d) $\{(x_1, x_2, \ldots, x_n) \mid x_1 = x_2 = \ldots = x_n = 0\}$;
(e) $\{(x_1, x_2, \ldots, x_n) \mid x_1 \in \mathrm{Z}\}$;
(f) $\{(x_1, x_2, \ldots, x_n) \mid x_1 \in \mathrm{Q}\}$;
(g) $\{(x_1, x_2, \ldots, x_n) \mid x_1 = -x_2\}$;
(h) $\{(x_1, x_2, \ldots, x_n) \mid 5x_1 + 3x_2 = 0\}$.

46. Let p be a prime number. How many vectors are there in the vector space $\mathrm{Z}_p, \mathrm{Z}_p^{1\times n}, +$?

47. Prove that the commutativity of addition in a vector space follows from the other axioms (clue: expand $(1 + 1)(v_1 + v_2)$ in two distinct ways).

48. The derivative

$$\mathrm{D} : \mathrm{R}[\mathrm{X}] \to \mathrm{R}[\mathrm{X}] : \sum_{i=0}^{n} a_i x^i \to \sum_{i=1}^{n} i a_i x^{i-1}$$

is a linear transformation of the vector space $\mathrm{R}, \mathrm{R}[\mathrm{X}], +$.

49. The primitive

$$\mathrm{S} : \mathrm{R}[\mathrm{X}] \to \mathrm{R}[\mathrm{X}]/\mathrm{R} : \sum_{i=0}^{n} a_i \mathrm{X}^i \to \sum_{i=0}^{n} \frac{a_i}{i+1} \mathrm{X}^{i+1} + \mathrm{R}$$

is a linear map of the vector space $\mathrm{R}, \mathrm{R}[\mathrm{X}], +$ into the vector space $\mathrm{R}, \mathrm{R}[\mathrm{X}]/\mathrm{R}, +$.

50. Let $\mathrm{A}, +, .$ be a ring. We have $\forall a, b \in \mathrm{A}$:

(a) $-(-a) = a$,
(b) $a.(-b) = -(a.b)$,
(c) $(-a).b = -(a.b)$,
(d) $(-a).(-b) = a.b$.

51. If

$$h : \mathrm{A}, +, . \to \mathrm{B}, +, .$$

is a homomorphism of rings, $h^{-1}(v)$ is an ideal of $\mathrm{A}, +, .$.

52. Let I be an ideal of the unitary ring $\mathrm{A}, +, .$. Prove that if $1 \in \mathrm{I}$, then $\mathrm{I} = \mathrm{A}$.

53. Let I be an ideal of the unitary ring $\mathrm{A}, +, .$. If I contains an invertible element of A, $\mathrm{I} = \mathrm{A}$.

54. The only ideals of a skew field $\mathrm{K}, +, .$ are K and $\{0\}$ (the trivial ideals).

55. What are the homomorphisms of a skew field into a ring (see Exercises 51 and 54)?

56. The set of integers $\{1, 3, 5, 7\}$ provided with the product modulo 8 is a group of order 4. To what group is it isomorphic?

57. Let a, b be elements of a group $\mathrm{G}, *$. Prove that if $a * b$ is of finite order, order $(b * a) =$ order $(a * b)$.

58. Express $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 5 & 2 \end{pmatrix} \in \mathscr{S}_6$ in terms of the generating subset $\left\{\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}\right\}$ of $\mathscr{S}_6$.

59. The set of matrices $\mathrm{R}^{m\times n}$ is a real vector space.
(The inner law is the matrix addition; the outer law is the multiplication of matrices by a real number.)

60. An inner law everywhere defined in a set E can be regarded as a function $\mathrm{E} \times \mathrm{E} \to \mathrm{E}$.
Every function $\mathrm{P} \to \mathrm{E}$ where $\mathrm{P} \subset \mathrm{E} \times \mathrm{E}$ is called an inner law inside E.
Subtraction is an inner law inside ω; it is not everywhere defined.
Subtraction is an inner law everywhere defined in Z.

61. The union of a chain of simple groups is a simple group.

62. The set of elements of $\mathscr{S}\{1, 2, 3, 4\}$ which leave invariant the polynomial $x_1x_2x_3 + x_4$ is a non-normal subgroup of order 6 of $\mathscr{S}_4$.

Is this group isomorphic to Z_6, $+$ or to the group $\mathscr{S}_3$, $\circ$?

63. Let G, $*$ be a group; let $g \in G$. Show that order (g) = order $(\bar{g})$.

64. Let G, $*$ be a group. If G contains only one element of order 2, this element belongs to the centre of G.

65. Give an example to show that the quotient of a group by its centre can have a centre $\neq \{\nu\}$

66. The quotient of a non-commutative group by its centre is not cyclic.

67. If the centre Z_G of the group G, $*$ consists of only one element, the centre of the group of automorphisms Auto (G) of G also reduces to a single element.

Solution: Let $f \in Z_{\text{Auto}(G)}$ (with f distinct from the identical automorphism), then there exists $g \in G$ such that $f(g) \neq g$. Since $f \in Z_{\text{Auto}(G)}$, f commutes with the inner automorphism $g.$:

$$f \circ g. = g. \circ f$$

i.e.

$$\forall x \in G: \quad (f \circ g.)(x) = (g. \circ f)(x)$$
$$\text{or: } \forall x \in G: \quad f(g.(x)) = g.(f(x))$$
$$\text{or: } \forall x \in G: \quad f(g * x * \bar{g}) = g * f(x) * \bar{g}$$
$$\text{or: } \forall x \in G: \quad f(g) * f(x) * f(\bar{g}) = g * f(x) * \bar{g}$$
$$\text{or: } \forall x \in G: \quad f(g) * f(x) * \overline{f(g)} = g * f(x) * \bar{g}$$

Then we have

$$\forall x \in G: \quad \bar{g} * f(g) * f(x) = f(x) * \bar{g} * f(g)$$

Now: (1) $\{f(x) \mid x \in G\} = G$ (since f is projective)

(2) $\bar{g} * f(g) \neq \nu$ (by hypothesis)

It follows that $\nu \neq \bar{g} * f(g) \in Z_G \neq \{\nu\}$.

Q.E.D.

68. Write down the quotient of the two groups of order 4 by a subgroup of order 2.

69. Prove that, up to isomorphism, there are only two groups of order 6: the cyclic group of order 6: Z_6, $+$ and the symmetric group of degree 3: $\mathscr{S}_3$, $\circ$.

70. Each of the two groups of order 6 contains one (and only one) normal subgroup isomorphic to Z_3, $+$. The quotient of Z_6 by this subgroup is isomorphic to the quotient of $\mathscr{S}_3$ by the subgroup in question.

71. A group G, $*$ is said to be complete if and only if
(a) $Z_G = \{\nu\}$.
(b) Every automorphism of G, $*$ is inner.
Show that every complete group is isomorphic to its group of automorphisms (see Revision exercises on Ch. 7, Ex. 87).

72. Normalizer

Let P be a subset of the group G, $*$. We define the normalizer of P in G, denoted by N_P, to be the set of elements of G which commute with P:

$$N_P = \{g \in G \mid g * P = P * g\}$$

Prove that N_P is the largest subgroup of G of which grp P is a normal subgroup.

73. If in the preceding definition we consider a subset P reduced to a single element: $P = \{p\}$, we call $N_{\{p\}}$ the normalizer of the element p and by an abuse of notation we write it N_p.

Prove that the normalizer of every element p of G contains the element p:

$$\forall p \in G: \quad p \in N_p$$

74. The normalizer of every subgroup S of G contains S: $S \subset N_S$.

75. Let P be any subset of Klein's four-group. $N_P = \ldots$?

76. Find the normalizer of sgp $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\}$ in $\mathscr{S}_3$.

77. (a) Find the normalizer of the element $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ in $\mathscr{S}_3$.

(b) Find the normalizer of sgp $\left\{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right\}$ in $\mathscr{S}_3$.

78. The normalizer of every subgroup S of G is the maximum subgroup of G in which S is normal.
From this deduce that: $N_s = G \Leftrightarrow \ldots$.

79. Centralizer

We define the centralizer Z_P of the subset P of the group G, $*$ to be the set of elements of G which commute with every element of P.

Hence

$$Z_P = \{g \in G \mid \forall p \in P: \quad g * p = p * g\}$$

Prove that Z_P is a subgroup of G, $*$.

80. Determine Z_P for every subset P of the four-group.

81. What is the centralizer of the following subsets of $\mathscr{S}_3$:

$$\operatorname{sgp}\left\{\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\}$$

$$\left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\}$$

$$\operatorname{sgp}\left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\}$$

82. As for the normalizer, we define the centralizer of an element p of the group G, $*$.

Prove that

(a) $\forall p \in G: \quad Z_p = N_p$;

(b) $\forall P \in \mathscr{P}G: \quad Z_P \subset N_P$.

(c) The centre of a group is the centralizer of the improper subset of the group.

83. Give an example to show that the centralizer of a subgroup of a group does not necessarily contain this subgroup.

84. Let P be a subset of the group G, $*$. Prove that

$$Z_P = \bigcap_{p \in P} N_p$$

85. Let S be a subgroup of the group G, $*$. Prove that Z_S is a normal subgroup of N_S.

86. The centralizer of a subset P of a group equals the centralizer of sgp P.

87. Denote by $Gl_2(R)$ the multiplicative group of real invertible 2×2 matrices. Show that

$$\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&-1\end{pmatrix}\right\}$$

is a subgroup of $Gl_2(R)$ which is not normal.

88. The centre of a group is a commutative subgroup of this group. Give an example to show that a commutative subgroup of a group is not necessarily contained in the centre of the group. (Clue: consider the simple group $\mathscr{A}_5, \circ$.)

89. Two subsets X, Y of the group G, $*$ are said to be *conjugate* and we then write $X \sim Y$ if and only if there exists an inner automorphism of G which maps X onto Y. We then have:

$$\forall X, Y \in \mathscr{P}G: \quad (X \sim Y) \Leftrightarrow (\exists g \in G: \quad g * X * \bar{g} = Y)$$

90. Show that the relation $\sim$ defined in the preceding exercise is an equivalence† defined in $\mathscr{P}G$.

All the elements of an equivalence class have the same cardinal.

91. Let X be a subset of the group G, $*$. Show that

$$\#\{P \in \mathscr{P}G \mid P \sim X\} = (G : N_X)$$

where $(G : N_X)$ is the index of the normalizer of X in G. (Clue: $g_1 * X * \bar{g}_1 = g_2 * X * \bar{g}_2 \Leftrightarrow g_1 * N_X = g_2 * N_X$. Deduce from this that the number of subsets conjugate to X is equal to the index of N_X in G.)

92. Two elements of the group G, $*$ are said to be conjugate if and only if this is so of the subsets containing a single element which they define. The relation thus defined in G is again denoted by $\sim$ and is an equivalence.

The class of the element x in this equivalence is a singleton $\Leftrightarrow$ $x \in Z_G$.

Two conjugate elements have the same order.

93. What is the partition defined by the group of inner automorphisms in the following groups:

(1) Klein's four-group;

(2) $\mathscr{S}_3, \circ$;

(3) the quaternion group.

94. A subset $P \neq \varnothing$ of a group G, $*$ is a subgroup of G if and only if P is a stable subset of G which contains the symmetric of each of its elements.

95. Let R, V, $+$ be a real vector space. Prove that

$$V \to R : v \to 0$$

is a linear map.

† Tr. See Appendix.

96. Let R, C^0, + be the real vector space of continuous functions with real values defined on the segment $[a, b] \subset R$.

Prove that the map

$$C^0 \to R : f \to \int_a^b f(t)\,dt$$

is a linear map.

97. The only homomorphism Q, + → Z, + is the null homomorphism. (Clue: consider the image of 1.)

98. There exists an epimorphism of the group Q_0^+, . onto the group Z, +. (Clue: every $q \in Q_0^+$ is of the form $2^z.q'$ where $z \in Z$ and 2 does not divide either the numerator or the denominator of q'.)

99. The set of prime numbers is a minimal generating subset of the group Q_0^+, ..

100. Every group with a finite generating subset is denumerable.

101. We have determined (Chapter 8) for every permutation a canonical decomposition into the product of transpositions. Prove that the number of transpositions in the canonical decomposition of a permutation is less than or equal to the number of transpositions in every decomposition of this permutation. (Clue: it is advisable to use the proof of the "parity" theorem.)

102. Let Ω, G, * be a commutative group with operators. Prove that the set of admissible endomorphisms of this group with operators is a subring of the ring of endomorphisms of the group G (see Revision exercises on Ch. 7, Ex. 106).

103. Let A, B be normal subgroups of the group G, *. Prove:

$$(A \cap B = \{\nu\}) \Rightarrow (\forall a \in A, \forall b \in B: \quad a * b = b * a)$$

(Clue: we have

$\forall a \in A, \forall b \in B: \quad a * b * \bar{a} \in B$ since B is normal; therefore:
$\forall a \in A, \forall b \in B: \quad a * b * \bar{a} * \bar{b} \in B$

Prove similarly that $a * b * \bar{a} * \bar{b} \in A$.)

104. Let G, * be a group. The order of every homomorphic image of G divides the order of G.

105. Denote by V the set of matrices

$$\left\{\begin{pmatrix} c & a - bi \\ a + bi & -c \end{pmatrix} \mid a, b, c \in R;\ i^2 = -1\right\}$$

(it is the set of 2 × 2 hermitian matrices of null trace).

Show that R, V, + is a (real) vector space.

Prove that the PAULI matrices

$$\left\{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right\}$$

form a minimal generating subset of this vector space.

Construct composition chains of R, V, +.

106. Let C be a normal chain of a group with operators Ω, G, *. Denote by $\mathscr{R}(C)$ the Schreier refinement of C. What can we say about $\mathscr{R}^2(C) = \mathscr{R}(\mathscr{R}(C))$?

107. A normal chain of a group G, * is strict if and only if the sequence of quotients of this chain does not contain a group isomorphic to $\{\nu\}$.

108. Every finite group is of finite dimension.

109. Principal chain.

Let Ω, G, * be a group with operators. Every composition chain of G

$$G = G_1 \supset G_2 \supset \ldots \supset G_n \supset G_{n+1} = \{\nu\}$$

such that

$\forall i \in \{1, 2, \ldots, n + 1\}$: G_i is a normal admissible subgroup of G, is called a principal chain of G. Show that if G admits a principal chain, 2 principal chains of G are equivalent (apply the Jordan-Hölder theorem by providing G with a suitable set of operators).

110. Define the concepts of a characteristic chain and an endostable chain of a group. Enunciate the corresponding Jordan-Hölder theorems.

111. In hamiltonian groups, the concepts of "composition chain" and "principal chain" are identical (see Revision exercises on Ch. 7, Ex. 57).

112. Solvable groups.

Denote by G′ the derived group of the group G, *. Denote further: $G'' = (G')', \ldots, G^{n+1} = (G^n)', \ldots$.

We say that the group G, * is solvable when there exists a $k \in \omega_0$ such that $G^k = \{\nu\}$.

113. Every subgroup of a solvable group is solvable.

114. Every quotient of a solvable group by a normal subgroup H is solvable. (Clue: prove that for every $n \in \omega$, $(G/H)^n \cong (H * G^n)/H$.)

115. If G, $*$ is a solvable group,

$$G \supset G' \supset G'' \supset \ldots \supset G^{k-1} \supset G^k = \{\nu\}$$

is a normal chain of G whose sequence of quotients consists of commutative groups (see Revision exercises on Ch. 7, Ex. 92, (c) and (g)).

116. If the quotient G/H of G by a solvable normal subgroup H is solvable, then G is solvable.

117. A group is solvable if and only if it admits a normal chain whose sequence of quotients consists of commutative groups.

118. Pick out the solvable groups amongst the following groups:

(a) Klein's four-group;
(b) $\mathscr{S}_3, \circ$;
(c) $\mathscr{S}_4, \circ$;
(d) $\mathscr{S}_5, \circ$;
(e) $\mathscr{S}_n, \circ$, with $n \geqslant 5$;
(f) the quaternion group;
(g) Z, $+$.

119. Let G, $*$ be a group. Study the law

$$\bar{*} : G \times G \to G : (x, y) \to x * \bar{y}$$

Is it everywhere defined, associative? Does it admit a left neuter, right neuter? Do there exist x, y such that

$$a \bar{*} x = b = y \bar{*} a$$

120. The group of isometries is not divisible.

121. Let G, $*$ be a group and $a \in G$. Prove that the law

$$T : G \times G \to G : (x, y) \to x * a * y$$

makes G into a group.

122. For what values of n is the group $\mathscr{S}_n, \circ$ divisible?

123. Let V, $+$ be the group of translations of the plane. Study the law

$$T : V + V \to V : (x, y) \to \tfrac{1}{2}(x + y)$$

Is it everywhere defined, associative, idempotent, commutative?
Show that the law T does not admit a neutral element.

124. Generalize Exercise 23 to the case of a group "with unique division" (see Chapter 3, §11).

125. Dihedral groups

Denote by S the set of vertices of a regular n-agon with centre 0. Let s be a symmetry with respect to a straight line containing 0 and and a vertex of the polygon.

Show that the set

$$Z_n \cup (s \circ Z_n)$$

is a subgroup of order $2n$ of $\mathscr{S}(S)$.

$Z_n \cup (s \circ Z_n)$ is called the dihedral group of order $2n$.

Z_n is a normal subgroup of the dihedral group of order $2n$.

The dihedral group of order $2n$ is isomorphic to the subgroup

$$\operatorname{sgp}\left\{\begin{pmatrix}1 & 2 & 3 & \ldots & n-1 & n\\ 2 & 3 & 4 & \ldots & n & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & \ldots & n-1 & n\\ n-1 & n-2 & n-3 & \ldots & 1 & n\end{pmatrix}\right\}$$

of $\mathscr{S}^n$.

126. Free group of a set.

Let E be a set. We propose to construct what we call the free group of E, the importance of which will be shown by Exercise 130.

To this end we first construct a set E^{-1} with the same cardinal as E and disjoint from E. We fix a bifunction

$$b : E \to E^{-1};$$

for every $x \in E$, we denote by x^{-1} the image $b(x)$ by the bifunction. The element x^{-1} is called the formal inverse of x and E^{-1} is the set of formal inverses.

We make the following definitions:

Definition 1. *Every finite sequence of letters of* $E \cup E^{-1}$ *is called a word.*

Definition 2. *The empty sequence is called the empty word and is denoted by* 1.

Definition 3. *Every word such that no letter x comes next to its formal inverse x^{-1} is called a reduced word.*

Definition 4. *The number of letters contained in a reduced word is called its length or degree.*

In particular the empty word is the only reduced word of degree 0.

Denote the set of reduced words in the letters of $E \cup E^{-1}$ by $\mathfrak{M}$. We make $\mathfrak{M}$ a group by providing it with the binary inner law of composition $\oplus$ defined as follows: given two reduced words M_1, M_2 we define the product of M_1 and M_2, denoted by $M_1 \oplus M_2$, to be the reduced word obtained by the juxtaposition of M_1 and M_2 and, when they arise, cancellations of $x \oplus x^{-1}$ and $x^{-1} \oplus x$.

Prove that $\mathfrak{M}$, $\oplus$ is a group. We call it *the free group of E* and denote it by $\mathscr{L}(E)$.

Note that for every $x \in E$, the inverse element of x in $\mathscr{L}(E)$ is equal to its formal inverse.

127. We define the rank of the free group of E to be the cardinal of E.

Every free group of finite rank is denumerable and the cardinal of a free group of infinite rank equals its rank.

128. Every free group of rank 1 is isomorphic to Z, +.

129. Every free group of rank >1 is non-commutative.

130. Every group is isomorphic to a quotient of a free group.

In fact let G, $*$ be a group and let P be a generating subset of G.

Denote the elements of P by $p_\alpha, p_\beta, \ldots$.

Let E be a set with the same cardinal as P. We fix a bifunction:

$$b : P \to E.$$

Prove that the map

$$h : \mathscr{L}(E) \to G : b(p_{\alpha_1}^{\varepsilon_1}) \oplus b(p_{\alpha_2}^{\varepsilon_2}) \oplus \ldots \oplus b(p_{\alpha_n}^{\varepsilon_n}) \to p_{\alpha_1}^{\varepsilon_1} * p_{\alpha_2}^{\varepsilon_2} * \ldots * p_{\alpha_n}^{\varepsilon_n}$$

(with $\forall i \in \{1, 2, \ldots, n\}$: $\varepsilon_i = \pm 1$) is an epimorphism of groups.

The homomorphism theorem for groups tells us that

$$\mathscr{L}(E)/h^{-1}(\nu) \cong G$$

131. Every group which admits a finite generating subset with n elements is isomorphic to a quotient of a free group of rank n.

Appendix

Throughout this work we use some logical symbols as abbreviations. Thus, $\Rightarrow$ means: "implies", and $\Leftrightarrow$ means: "if and only if". We make systematic use of the logical symbols $\forall$ (for every) and $\exists$ (there exists).

We sometimes use the symbol $\ni$— for "such that".

We indicate that the element a belongs to the set E, by writing $a \in E$. If the contrary is true we write $a \notin E$.

The expression $A \subset B$ signifies that the set A is included in the set B, i.e. that every element of A is an element B.

If $P \subset E$, we say that P is a subset of E, and $\mathscr{P}E$ denotes the set of subsets of E.

The term $A \cap B$ denotes the intersection of the sets A and B, i.e. the set of elements which belong at the same time to A and to B.

The term $A \cup B$ denotes the union of the sets A and B, i.e. the set of elements which belong to one (at least) of the sets A and B.

The term $A \setminus B$ denotes the set of elements of A which are not elements of B.

We put $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

The empty set is denoted by $\varnothing$.

The term $\{x \mid P(x)\}$ reads "the set of x such that $P(x)$" and denotes the set of elements x satisfying the property P.

By $\{a, b, c\}$ we mean the set formed by the elements a, b, c.

We denote by (a, b) the pair with origin a and end-point b. Thus

$$(a, b) = (c, d) \Leftrightarrow (a = c \text{ and } b = d)$$

The pair (b, a) is called the inverse of the pair (a, b).

A relation r is defined as a set of pairs; its domain is the set of origins of its pairs and its image is the set of their end-points.

In particular $A \times B$ is the set of pairs whose origins belong to A and whose end-points belong to B.

A relation of A to B is a subset of $A \times B$.

A function $f : A \to B$ (or map of A into B) is a relation of A to B such that every element of A is the origin of one and only one pair of f.

The inverse r^{-1} of the relation r is the set of inverses of pairs of r.

A function $f : A \to B$ is said to be injective if and only if no element of B is the end-point of two distinct pairs of f. (We then say f is an injection.)

A function $f : A \to B$ is said to be projective if and only if every element of B is the end-point of (at least) one pair of f.

A function $f : A \to B$ is called a bifunction or bijection if and only if f^{-1} is a function $B \to A$, i.e. if and only if f is at the same time injective and projective.

We define the product of the relations r and s to be the relation defined by

$$s \circ r = \{(a, c) \mid \exists b : (b, c) \in s \quad \text{and} \quad (a, b) \in r\}$$

i.e. the set of pairs (a, c) for which there exists an element b such that (a, b) is a pair of r and (b, c) a pair of s.

By a transformation of a set E we mean every function $E \to E$.

By a permutation of a set E we mean every bifunction $E \to E$.

If $f : A \to B$, we denote by $f(a)$ the end-point of the pair of f having a as origin. The element $f(a)$ is the value of f at a or the image of a by f.

If $f : A \to B$ and $g : B \to C$, we have $(g \circ f)(a) = g(f(a))$; thus $g \circ f = \{(a, g(f(a)) \mid a \in A\}$.

If $P \subset A$, the set of images by f of the elements of P is called the image of P by f and we denote it by fP.

Thus $fP = \{f(p) \mid p \in P\}$.

For every $Q \subset B$ we put $f^{-1}Q = \{x \in A \mid f(x) \in Q\}$.

We say that $f^{-1}Q$ is the inverse image of Q by f.

If there exists a bifunction $A \to B$ we say that the sets A and B are equipotent, or that they have the same cardinal, and we write $\# A = \# B$.

The above notations have been used very flexibly, and we have allowed ourselves some abuses of notation and language as described in the text.

TRANSLATOR'S APPENDIX

A set which is equipotent with the set ω of natural integers is said to be denumerable.

The expression $f : A \times B \to C : (a, b) \to f(a, b) = c$ reads "the function f of $A \times B$ to C maps the element $(a, b) \in A \times B$ to the element $f(a, b) = c \in C$".

Let S be a set.

A partition Π of S is any collection of subclasses A, B, C, . . . of S such that each element of S belongs to one and only one of the subclasses of the collection.

A relation $x \sim y$, defined in S, and which is

1. reflexive, i.e. $x \sim x$ for all $x \in S$.
2. symmetric, i.e. $x \sim y \Leftrightarrow y \sim x$,
3. transitive, i.e. $(x \sim y \text{ and } y \sim z) \Rightarrow x \sim z$ is called an equivalence.

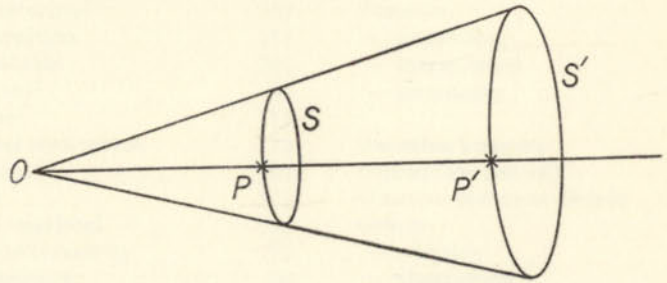
It defines a partition of S into equivalence classes. x and y belong to the same equivalence class if and only if $x \sim y$.

The relation $<$ is anti-symmetric if and only if $(x < y \text{ and } y < x) \Rightarrow x = y$.

A (partial) ordering is reflexive, anti-symmetric and transitive. A set provided with a (partial) ordering $<$ is called a (partially) ordered set.

A (partially) ordered set S such that for every $x, y \in S$, either $x < y$ or $y < x$ is called a totally ordered set, and the relation $<$ is then said to be a total ordering.

A lexicographic ordering of a set a_{ij} is defined as follows: $a_{lm} < a_{rs}$ whenever l comes before r in the alphabet. If $l = r$, then $a_{lm} < a_{ls}$ if m comes before s in the alphabet.



Let O be a fixed point. If P is a variable point on a fixed curve S and P′ is a point on OP such that $\frac{OP'}{OP} = k$ (constant), then the locus of P′ is a curve S′ which is said to be homothetic to S. See the diagram. Such a relation is called a homothety or similarity. O is the centre of similitude. If $k = 0$, S′ coincides with the point O. This is called the constant homothety.

Terminological Index

Absorbent 25
Admissible homomorphism 160
— subgroup 157
Algebraic structure 1
A-module 155
Antisymmetric 55
Artin's condition 191
Associativity 2
— mixed 34
Autodistributivity 22
Automorphism 93
— inner 103

Bifunction 212
— canonical 97
Bijection 212

Cancellation 11
Cardinal 212
Cayley table 28
Centralizer 203
Centre 27
Chain 171
— characteristic 207
— composition 174
— endostable 207
— maximal 50
— normal 172
— normal equivalent 173
— principal 207
— strict 171
— strict maximal 171
Commutassociativity 23
Commutativity 10
Commutator 121
Compatible (law and relation) 64
Conjugate elements 205
Conjugate subsets 205
Cycle 135
Cyclic group 44

Denumerable 212
Dilatation 106
Dimension (of a vector space) 171
— (of a group) 177
Direct product 26
— sum 26
Distributivity 65
Divisors 67
Domain 126

Element 1
— Central 103
— invertible 69
— symmetrizable 22
Endomorphism 93
Epimorphism 90
Equality 12
Equipotent 212
Equivalence 213
Equivalent chains 173
— sequences 173
Exact sequences 122
Expanding function 44

Field 156
Filtering (set) 80
Four-group 29
Function 211
— expanding 44
— idempotent 44
— increasing 44

Gaussian integers 87
Generators (set of) 44
Greatest common divisor 74
Group 3
— additive 12
— alternating 143
— commutative 10
— complete 203
— cyclic 44
— dihedral 209
— divisible 35
— free 209
— hamiltonian 57
— multiplicative 12
— ordered 64
— quaternion 28
— simple 143

Group—*continued*
— solvable 207
— symmetric 19
— with operators 150

Highest common factor 74
Homomorphism 90
— admissible 160
— theorem 98
Ω-homomorphism 161
Homothety 213

Ideal 157
Idempotent 7
Image 94
Increasing function 44
Index of a subgroup 49
Infimum 55
Injection 212
Integers 13
— modulo n 18
Intersection 211
Inverse 13
— formal 209
Isometry 106
Isomorphism
— of groups 91
— of ordered sets 82
— theorems 106

Kernel 101
Klein's four-group 29

Ladder 179
Lattice 57
— modular 118
Law 1
— admitting cancellation 62
— everywhere defined 1
— induced 99
— inner 1
— inverse 9
— outer 30
— scalar 31
Length of a reduced word 209

Map 211
— linear 161
Modular theorem (Dedekind) 60

Module 55
Monomorphism 90
Moore's closure 43

Neuter 3
Noether's condition 190
Normal equivalent chains 173
Normalizer 203

Operators (set of) 150
Order of an element 54
— of a group 49
— of minimal permutation 133
Ordering 55
— total 64
— lexicographic 213

Partition 213
Pauli matrices 207
Permutation 19
— denumerable 132
— even 142
— minimal 128
— odd 142
Polynomials 88
Primary (number) 79
— maximal 82
Primary factorization 80
Prime (number) 69
Prime factorization 77
Product
— of relations 212
— of sets 212
— of subgroups 55
— of subsets 99
Projection 212

Quaternion 198
Quotient of a group by a homomorphism 97
Quotient-group
— by a homomorphism 98
— by a normal subgroup 104

Rank of a free group 210
Rationals 13
Real vector space 156
Reals modulo 1 17

Refinement 176
Relation 211
Ring 66
— of endomorphisms of a commutative group 122
— euclidean 70
— factorial 75
— — module 155
— of operators 155
— ordered 66
— of polynomials 88
— of rational integers 66

Scalar multiplication 151
Separation 179
Set 1
— of operators 150
Skew field 156
Step 179
Subgroup 38
— admissible 157
— characteristic 118
— central 103
— endostable 118
— generated by P 42
— improper 41
— invariant 120
— maximum 41
— minimum 41
— normal 101
— periodic 119
— trivial 41
Submodule 56
— cyclic 72
Sub-permutation 127
Subset 211
— generating 42
— stable 38
Sum of submodules 56
Supremum 56
Symmetric 5
— difference 19
— group 19
Symmetrizable (element) 22

Ternary cycle 143
Theorems
— Euclid's 72
— homomorphism
(groups) 98
(groups with operators) 163
— first isomorphism
(groups) 106
(groups with operators) 166
— second isomorphism
(groups) 107
(groups with operators) 167
— Lagrange's 49
— modular (Dedekind) 60
— Jordan–Hölder 175
— four-set 182
— four-groups 188
— Schreier's 177
— Zassenhaus' 188
Transformation of a relation 105
Transposition 125

Union 211

Vector space 156
Vector subspace 158

Word 209
— empty 209
— reduced 209

List of Plates

Plate 1 The symmetric difference of A and B is represented by the areas surrounded by the red line.
(See Ch. 2, §5 (f).)

Plate 2 A $\triangle$ B is surrounded by the red line, B $\triangle$ C by the blue line, and (A $\triangle$ B) $\triangle$ C = A $\triangle$ (B $\triangle$ C) by the green line.
(See Ch. 2, §5 (f).)

Plate 3 An exercise on the solubility property of groups. Find the subset X of E such that A $\triangle$ B = B.
(See Ch. 1, §3 (c).)

Plate 4 The solution of the problem posed in plate 3. X is the set surrounded in red.
(See Ch. 2, §5 (f).)

Plate 5 A diagrammatic representation of the law of combination of a permutation group. An element of the group is represented by a permutation of the points .. The green lines represent the permutation f; the blue lines represent g, and the brown lines represent the composite permutation $h = g \circ f$.
(See Ch. 2, §5 (g) and Ch. 8.)

Plate 6 The group solubility property for a permutation group.
(See Ch. 2, §5 (g).)

Plate 7 A representation of Klein's four-group as the group whose elements are semi-rotations about the three axes shown together with the identical rotation. In the Cayley table the rotations are represented by coloured dots.
(See Revision ex. on Ch. 1 and 2, Ex. 41 (e).)

Plate 8 A representation of Klein's four-group as a permutation group whose elements are represented by the red, green and blue lines and the yellow identical permutation.
(See Plate 7. Revision ex. on Ch. 1 and 2, Ex. 41 (e).)

Plate 9 The plane is made into a group V, + by choosing an arbitrary point O in it as origin. Each point P of the plane now represents a vector with origin O and end-point P.
(See Ch. 5, §5. Ch. 7, Ex. 109 (3).)

Plate 10 An illustration of addition and subtraction in V, + by the parallelogram law of combination of vectors.
(See Ch. 5, §5.)

Plate 11 Five subgroups of V, + represented by different colours.
A subgroup generated by a line must consist of parallel lines in order to ensure stability under the parallelogram law of addition.
The sum of two points collinear with the origin is also collinear with them.
Each subgroup must contain the origin, i.e. the neutral element.

Plate 12 Verify that the red spots form a subgroup of V, +.
(See Ch. 4, §1.)

Plates 13–22 Exercises and examples on various aspects of group theory applied to the group V, +.

Plate 23 The elements of the quotient group V/S are lines parallel to S.
(See Ch. 7, §10.)

Plate 24 Addition in V/S. S is represented by the brown lines.
Use the parallelogram law.

Plate 25 The negative of an element of V/S.

Plate 26 Cayley tables for the two groups of order 4.
(See Revision ex. on Ch. 1 and 2, Ex. 41 (e).)

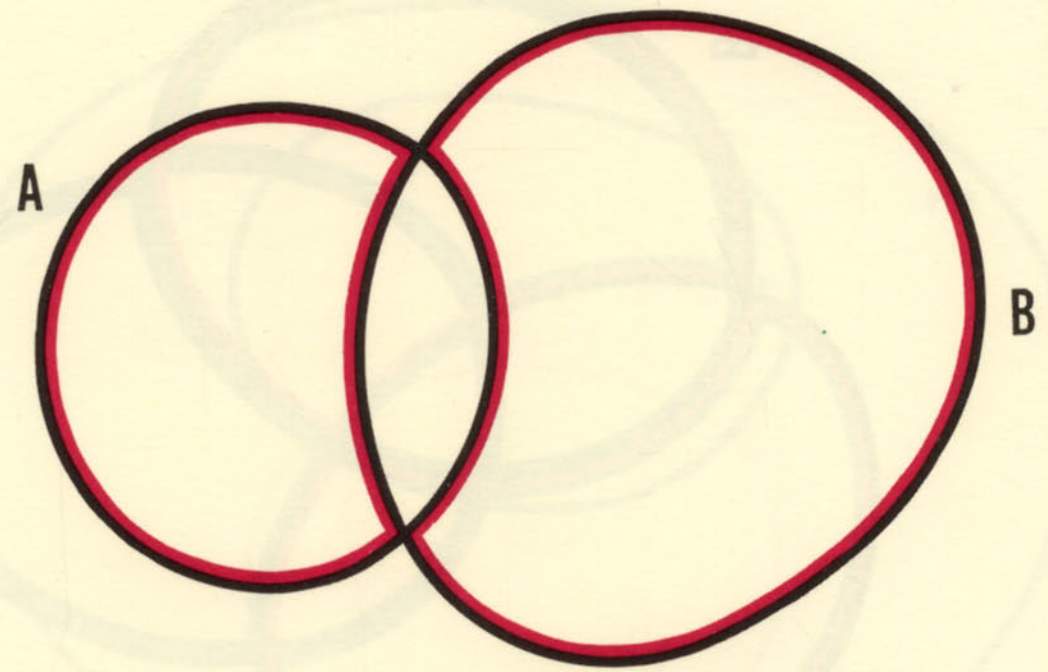
Plate 27 A representation of the symmetric group of three elements.
(See Ch. 8.)

Plate 28 Cayley table for the previous group.

Plate 29 A representation of a cycle (brown lines) as a product of transpositions (yellow, green, light blue, orange and dark blue lines).
(See Ch. 8.)

Plate 30 Some products of cycles.

Plates 31–32 Illustrations of some of the properties of sets used in Ch. 10.

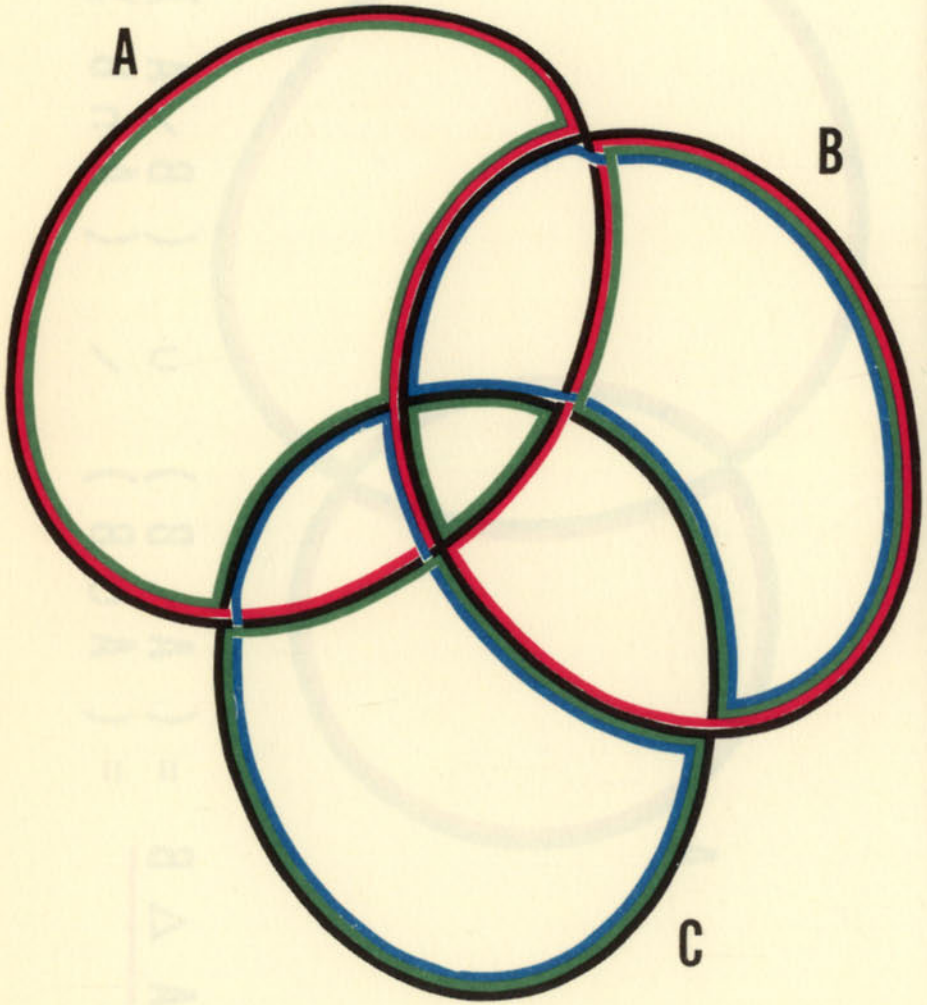


$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$
$$= (A \cup B) \setminus (A \cap B)$$

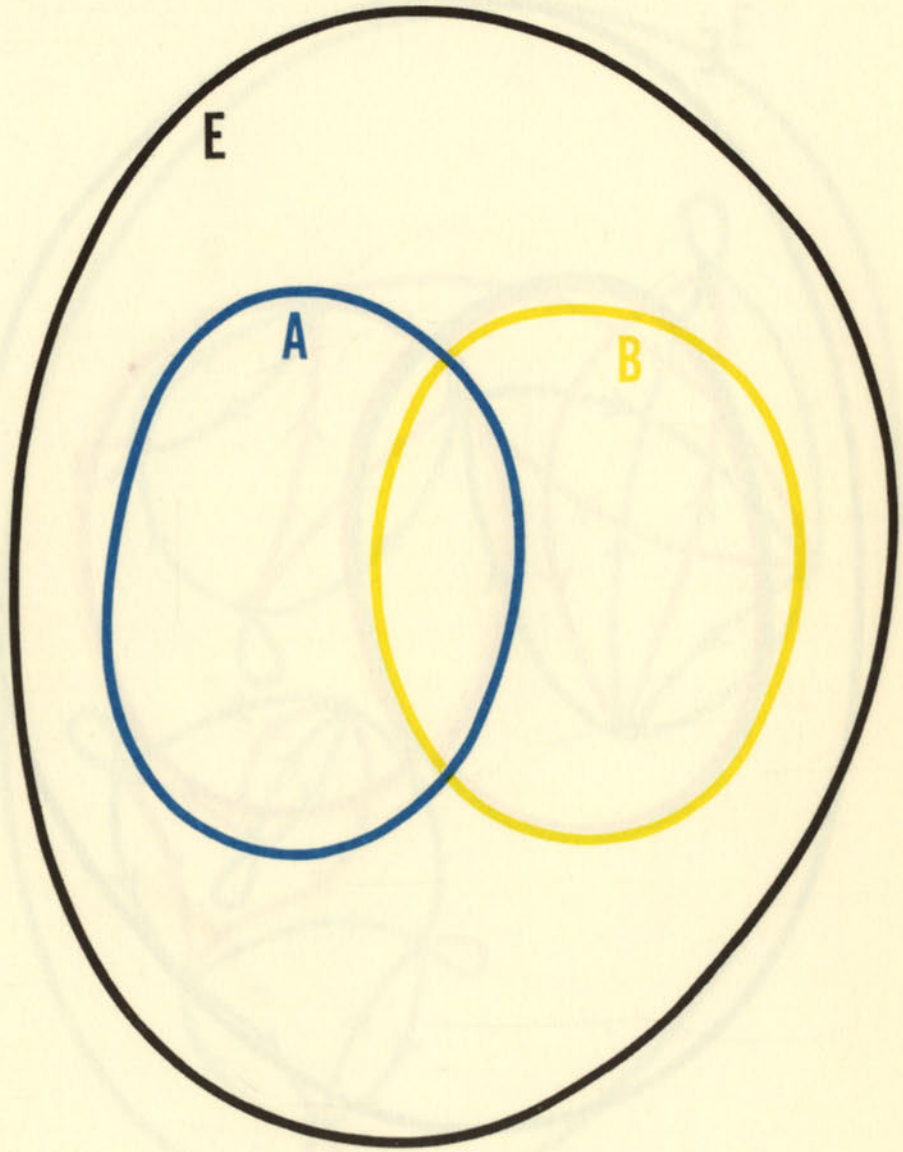
The symmetric difference

Plate 1

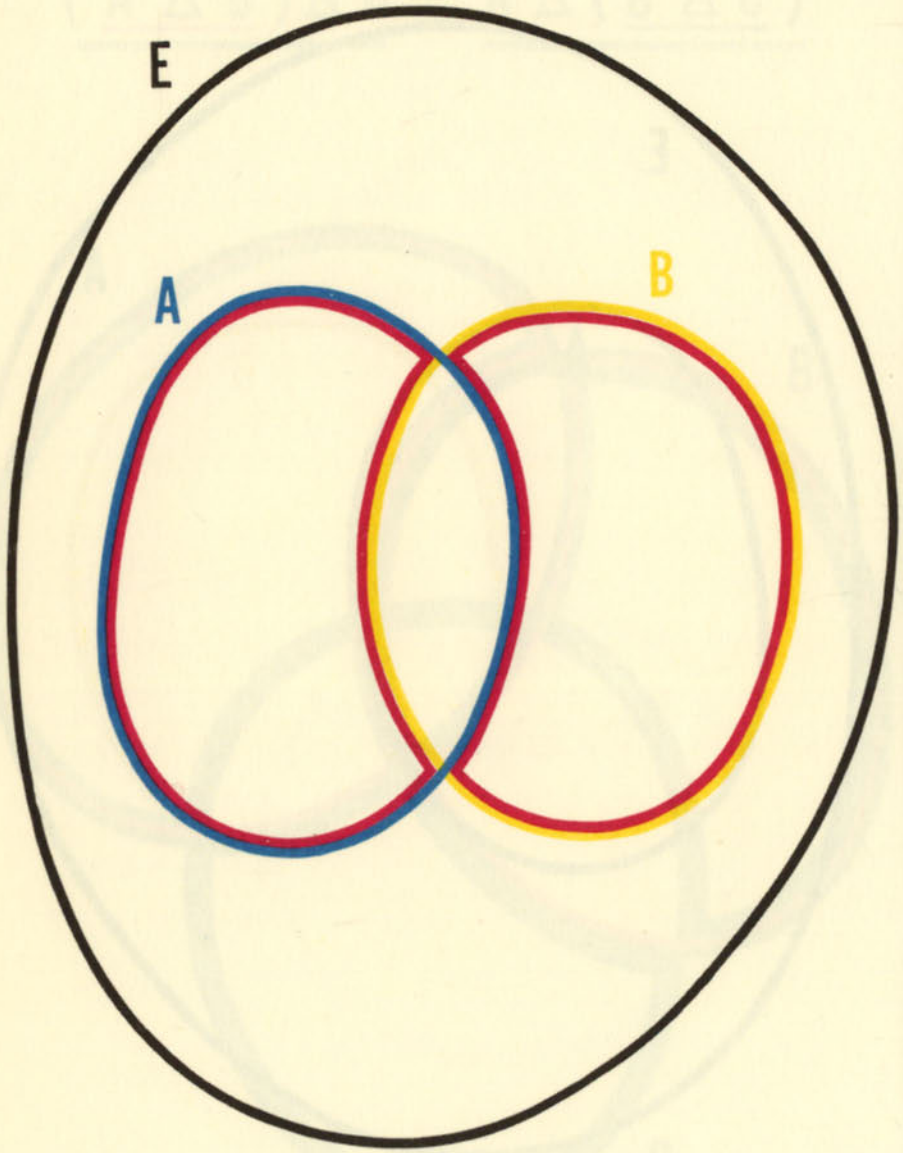
$$(A \triangle B) \triangle C = A \triangle (B \triangle C)$$



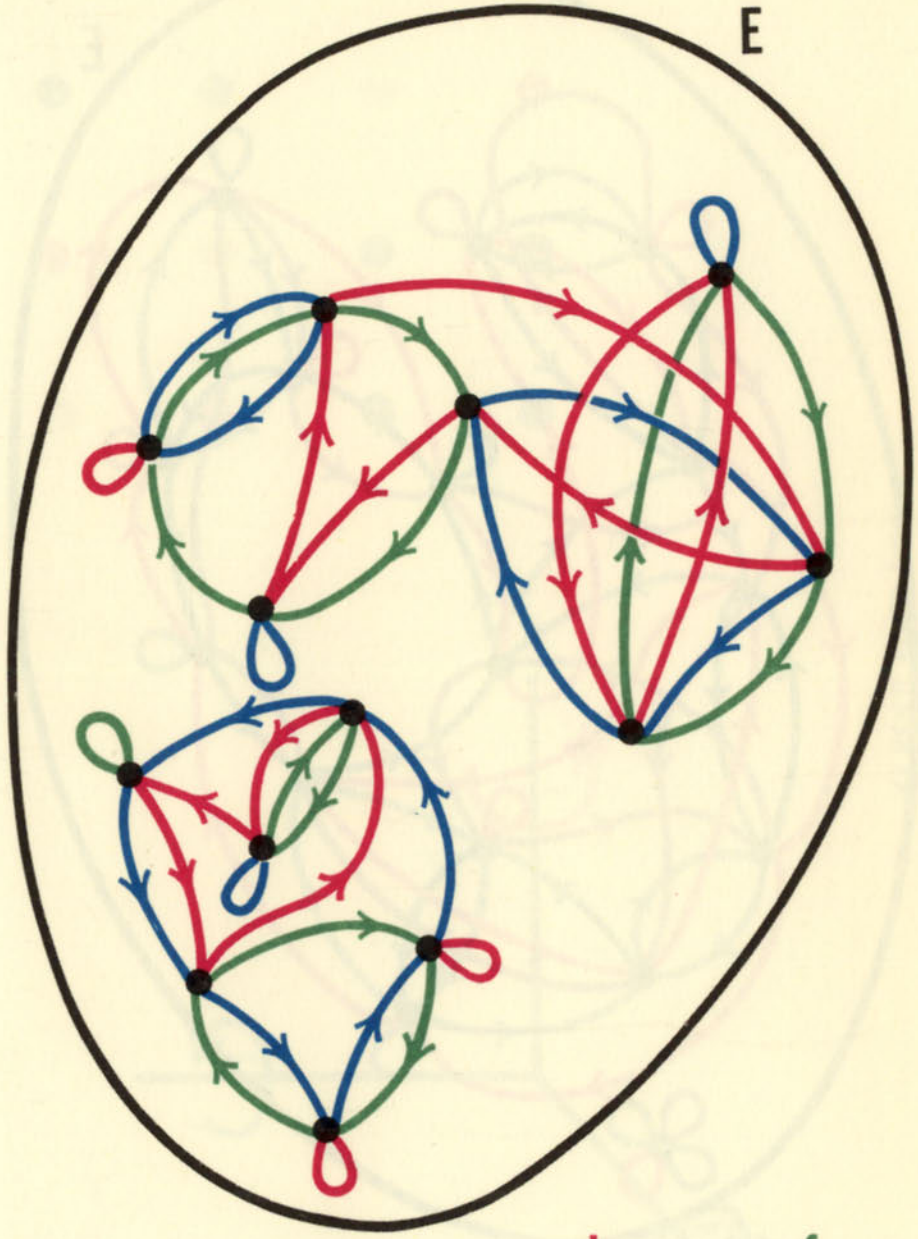
Associativity of the symmetric difference

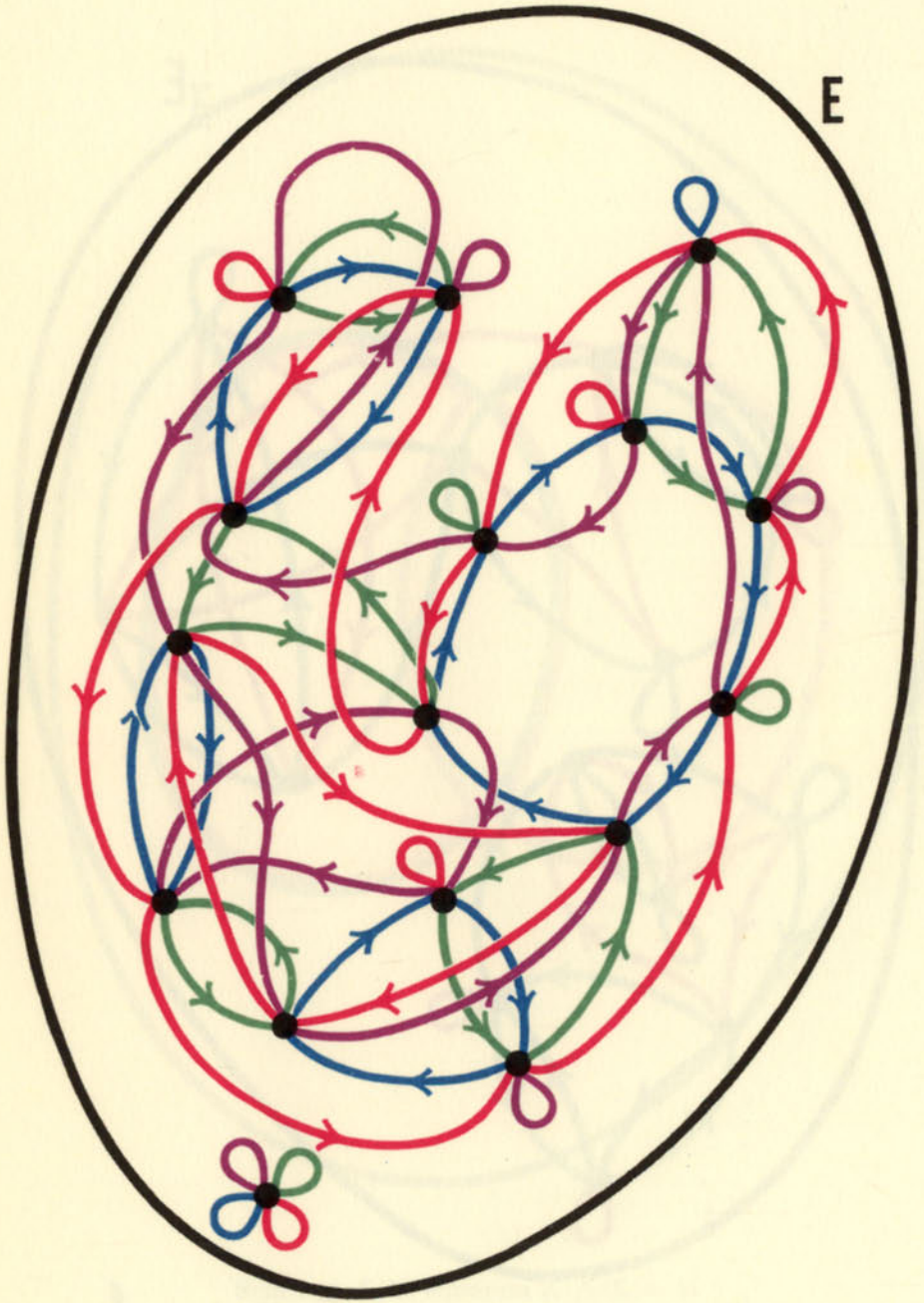


In $\mathscr{P}$E, $\triangle$ solve the equation $A \triangle X = B$

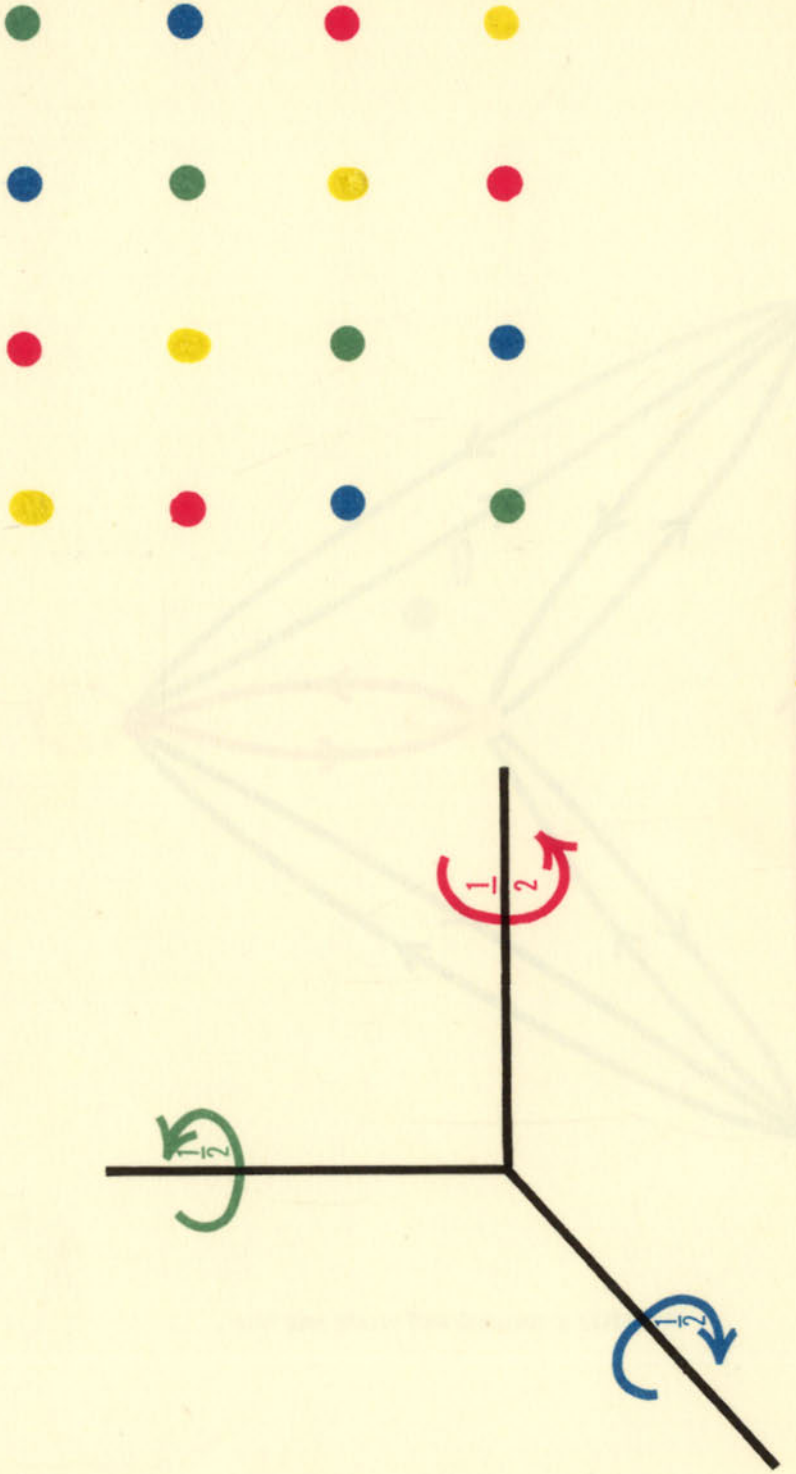


Solution of the equation A $\triangle$ X = B

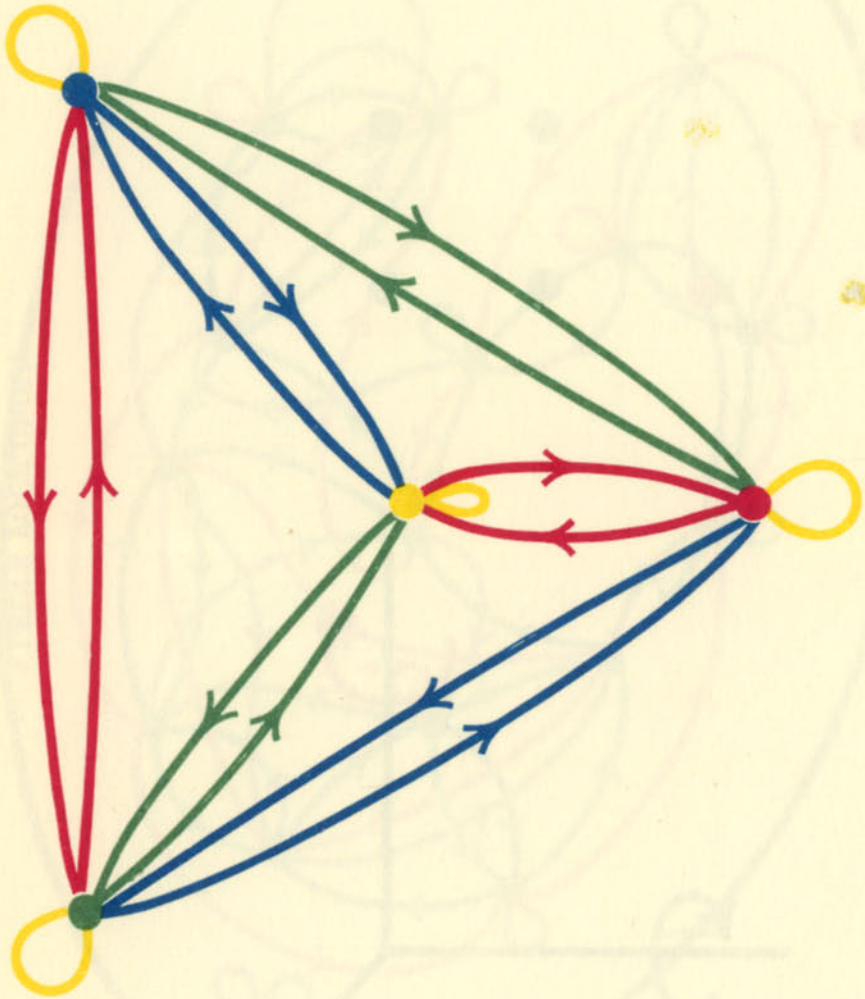




$$\forall a, b \in \mathcal{S}_E, \exists x, y : a \circ x = b = y \circ a$$



KLEIN'S FOUR-GROUP

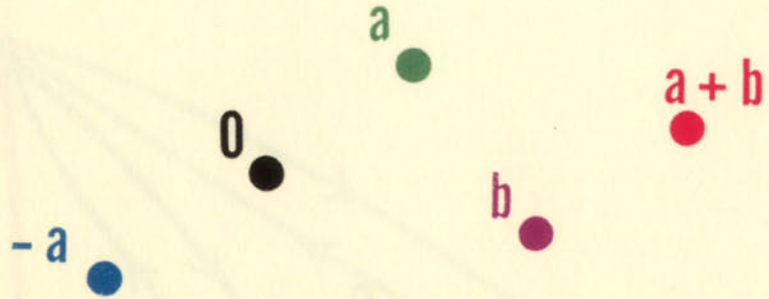


KLEIN'S FOUR-GROUP

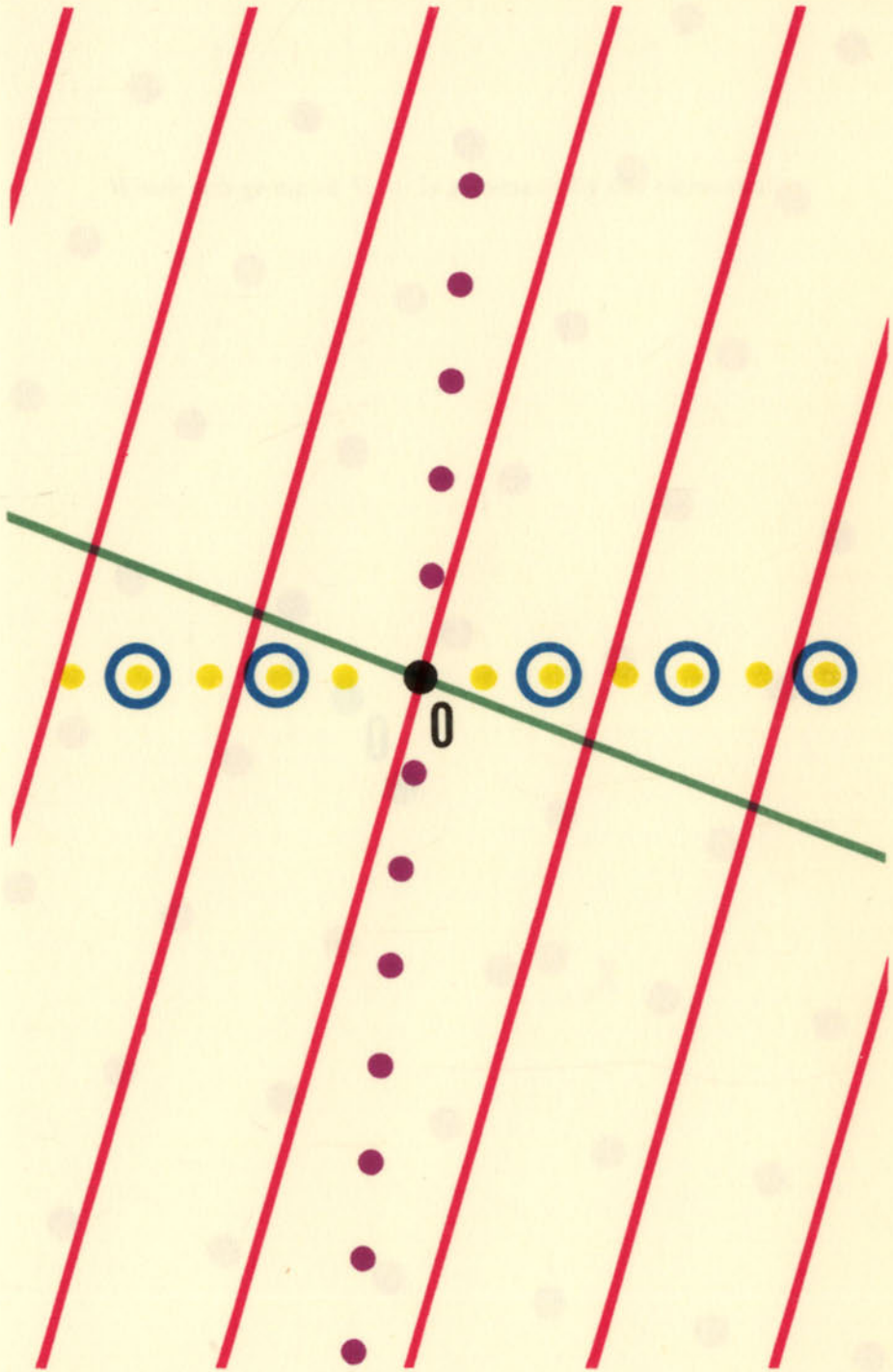
0

. . . and the plane has become a GROUP

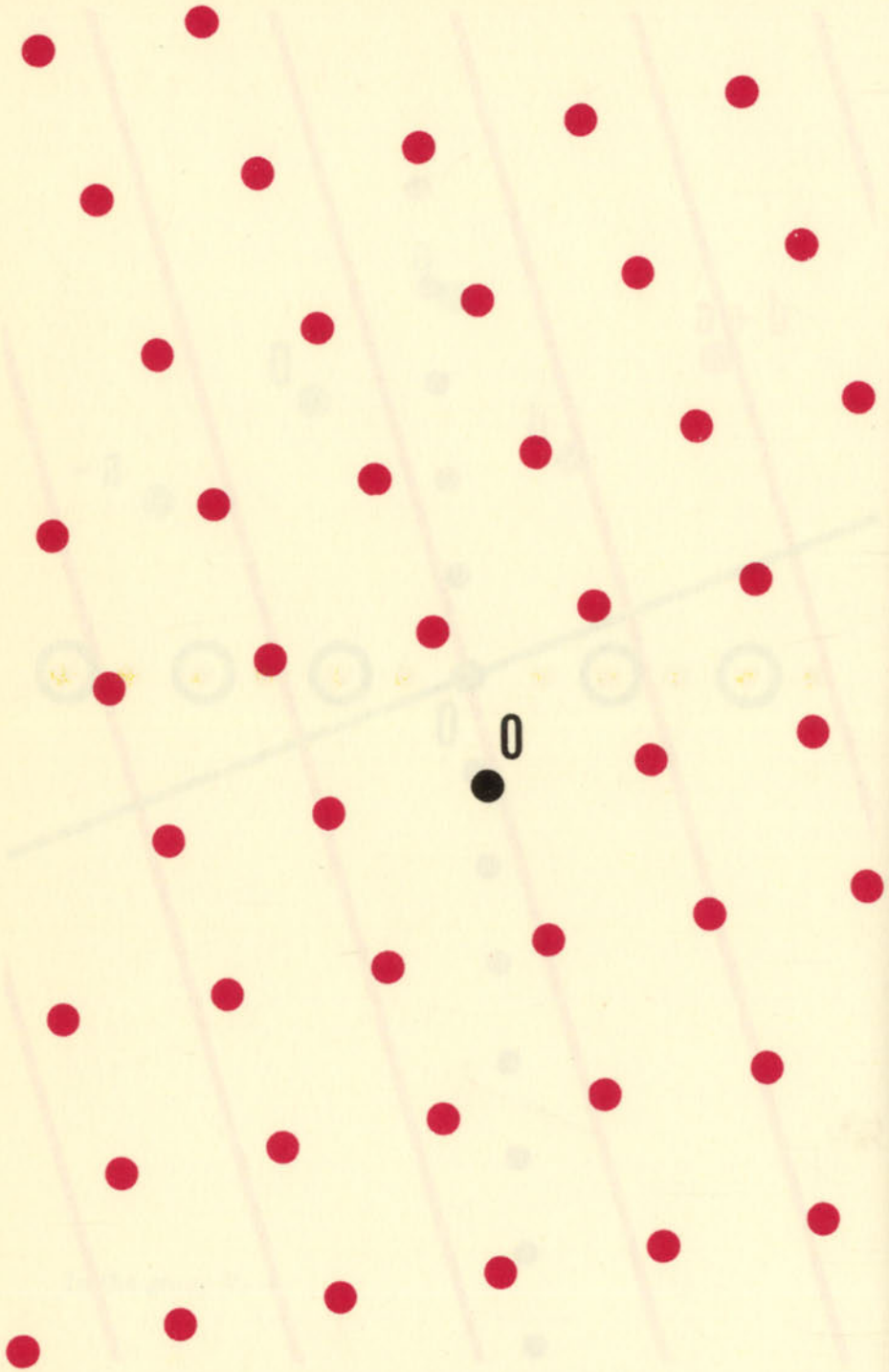
V, +



In the group V, +

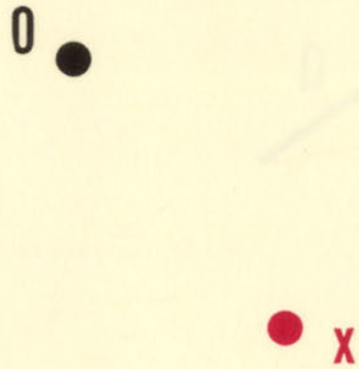


Some sub-groups of V, +

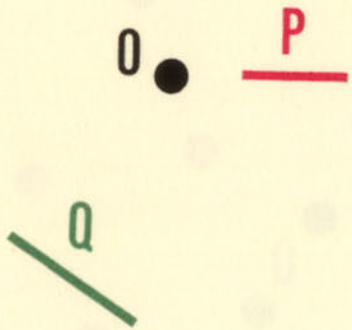


Another sub-group of V, +

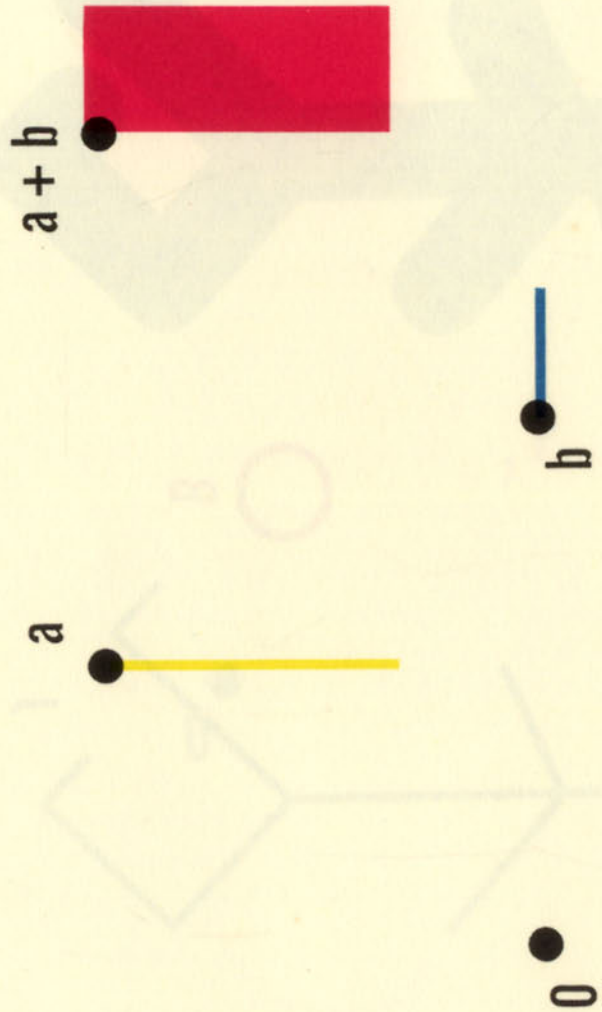
Which sub-group of V, + is generated by the element x?



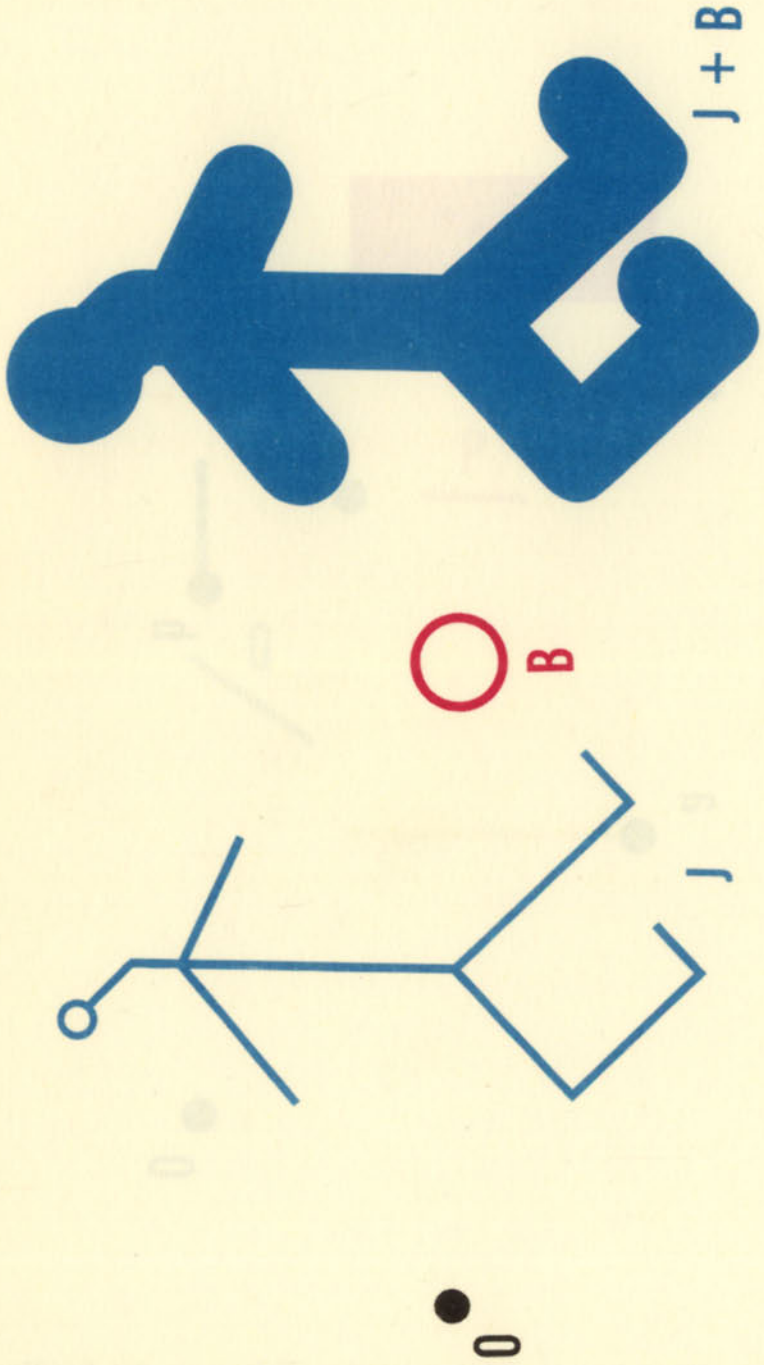
Which sub-group of V, + is generated by the subset P?



Which sub-group of V, + is generated by the subset Q?

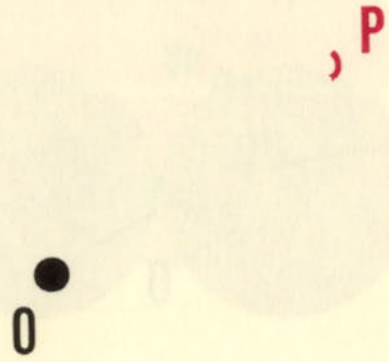


In V, +

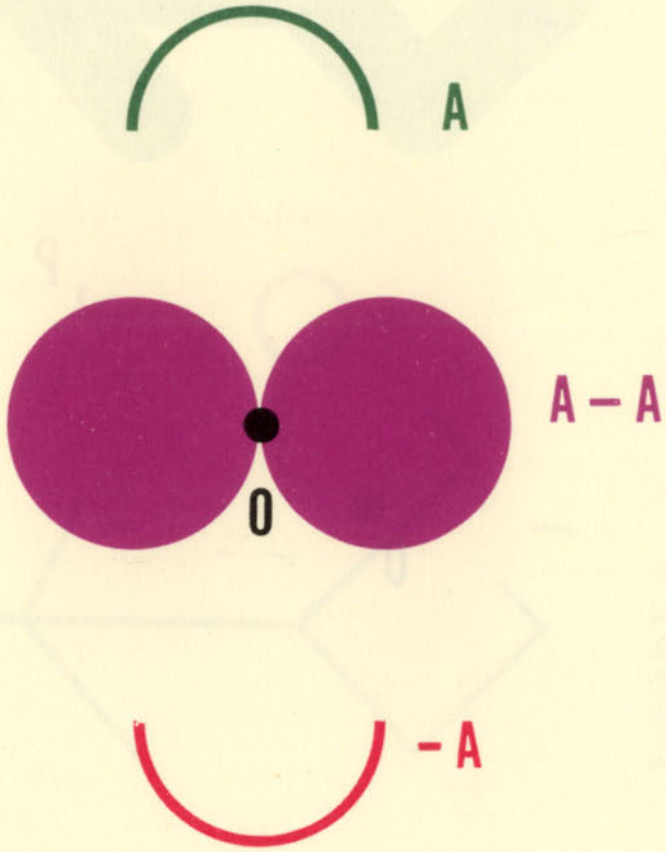


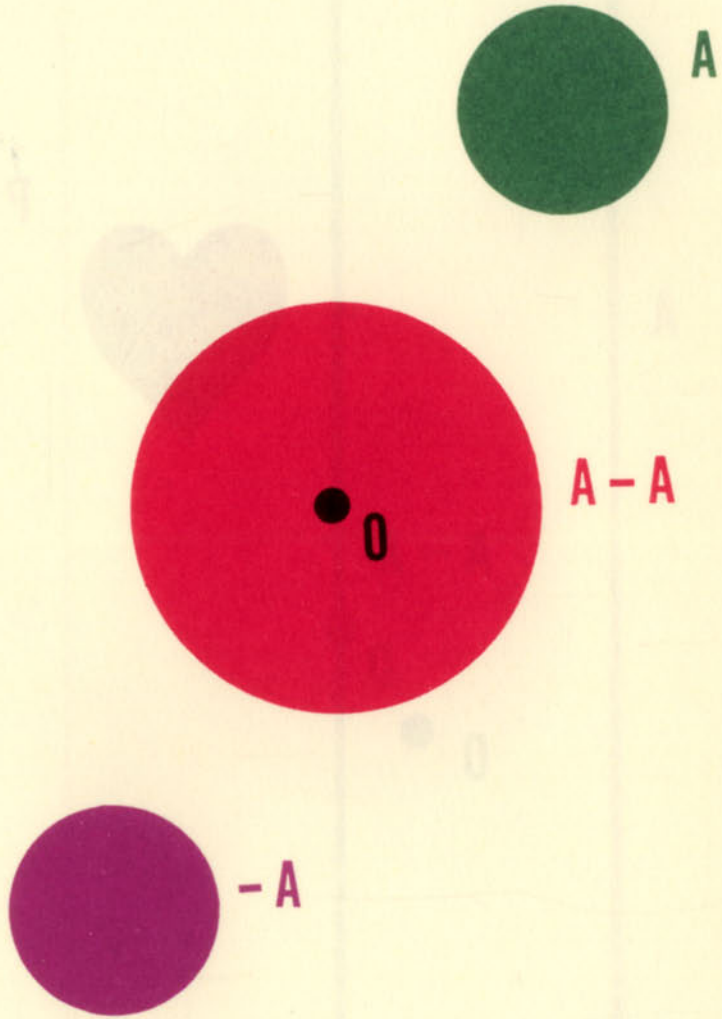
Football in V, +

Which sub-group of V, + is generated by the subset P?



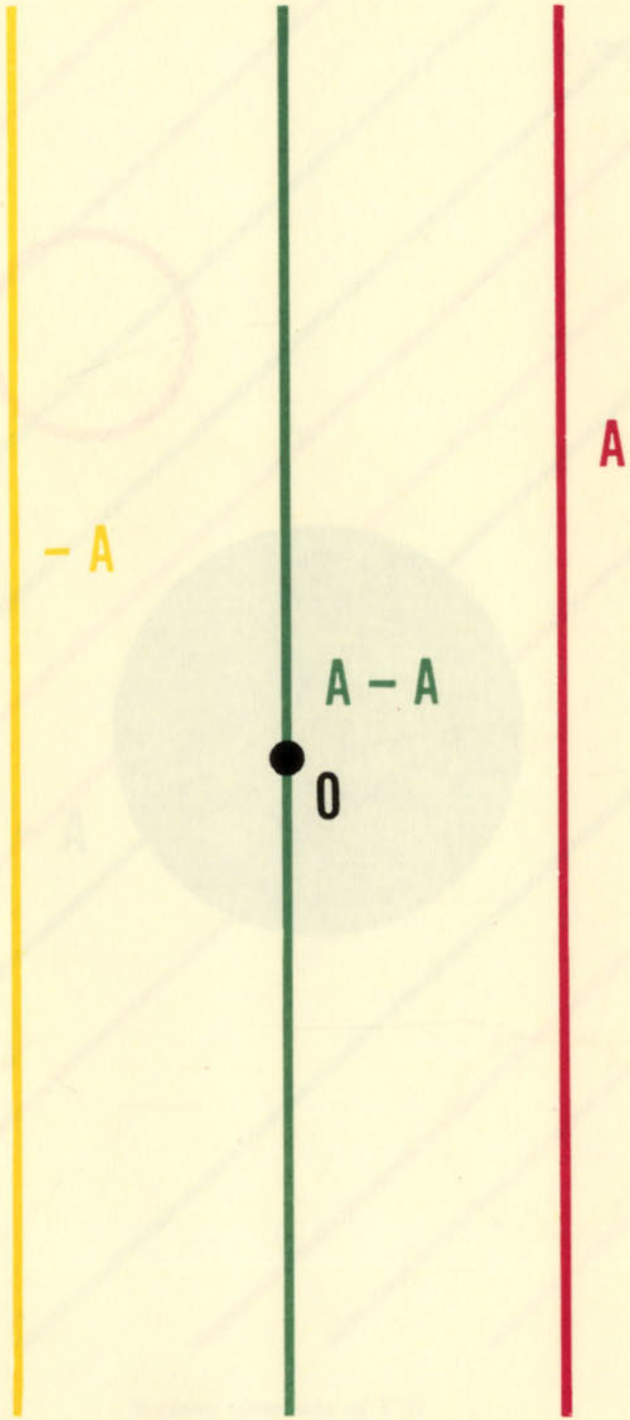
In V, +



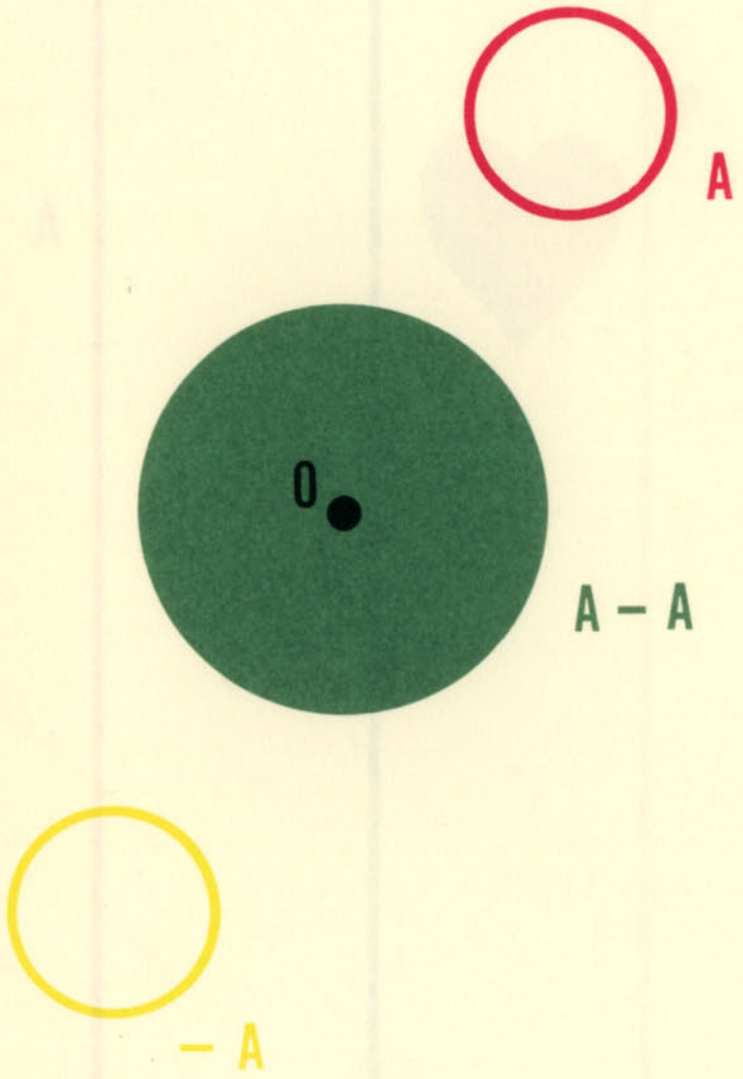


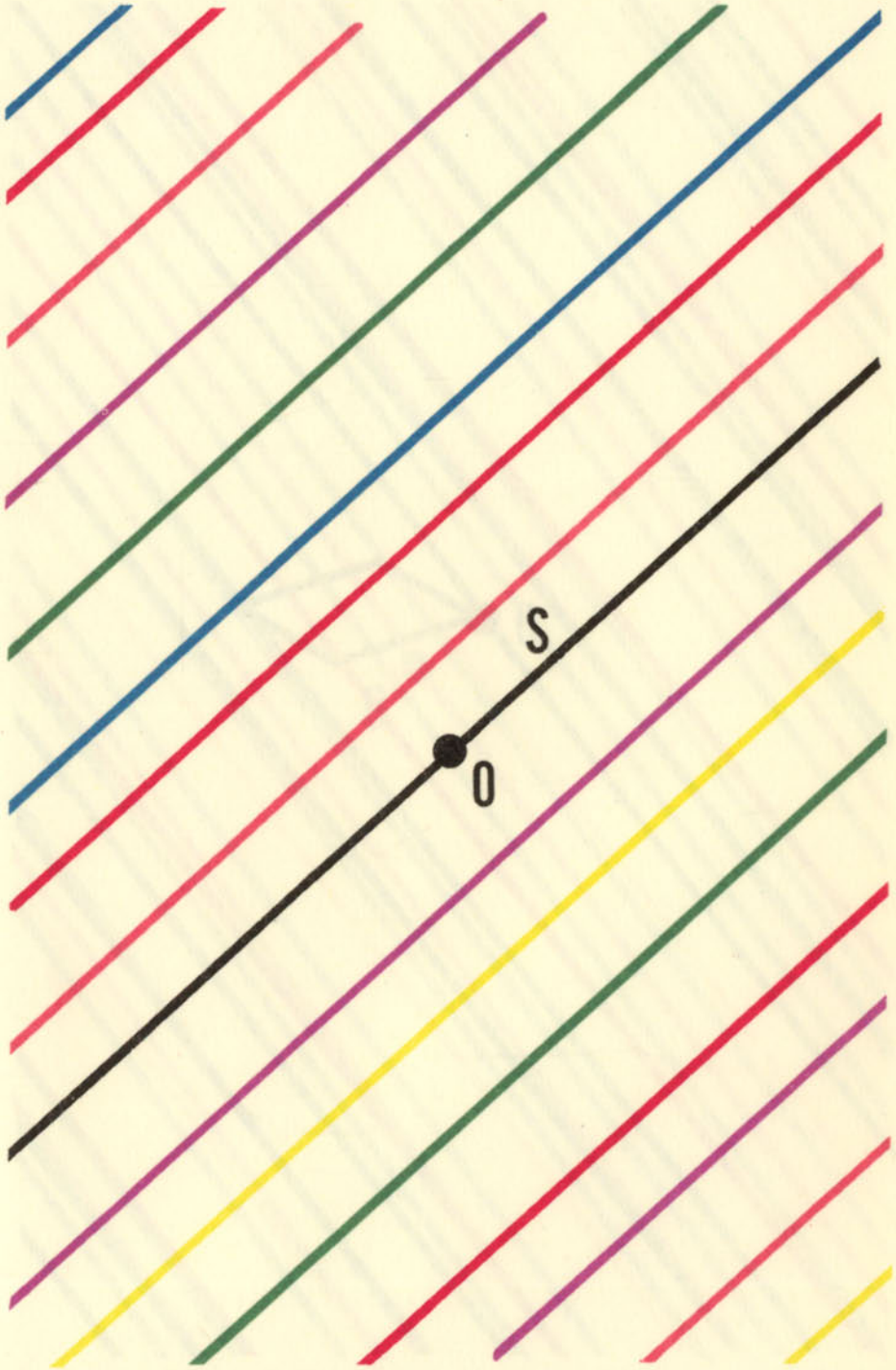
Which sub-group of V, + is generated by the subset P?

In the group V, +

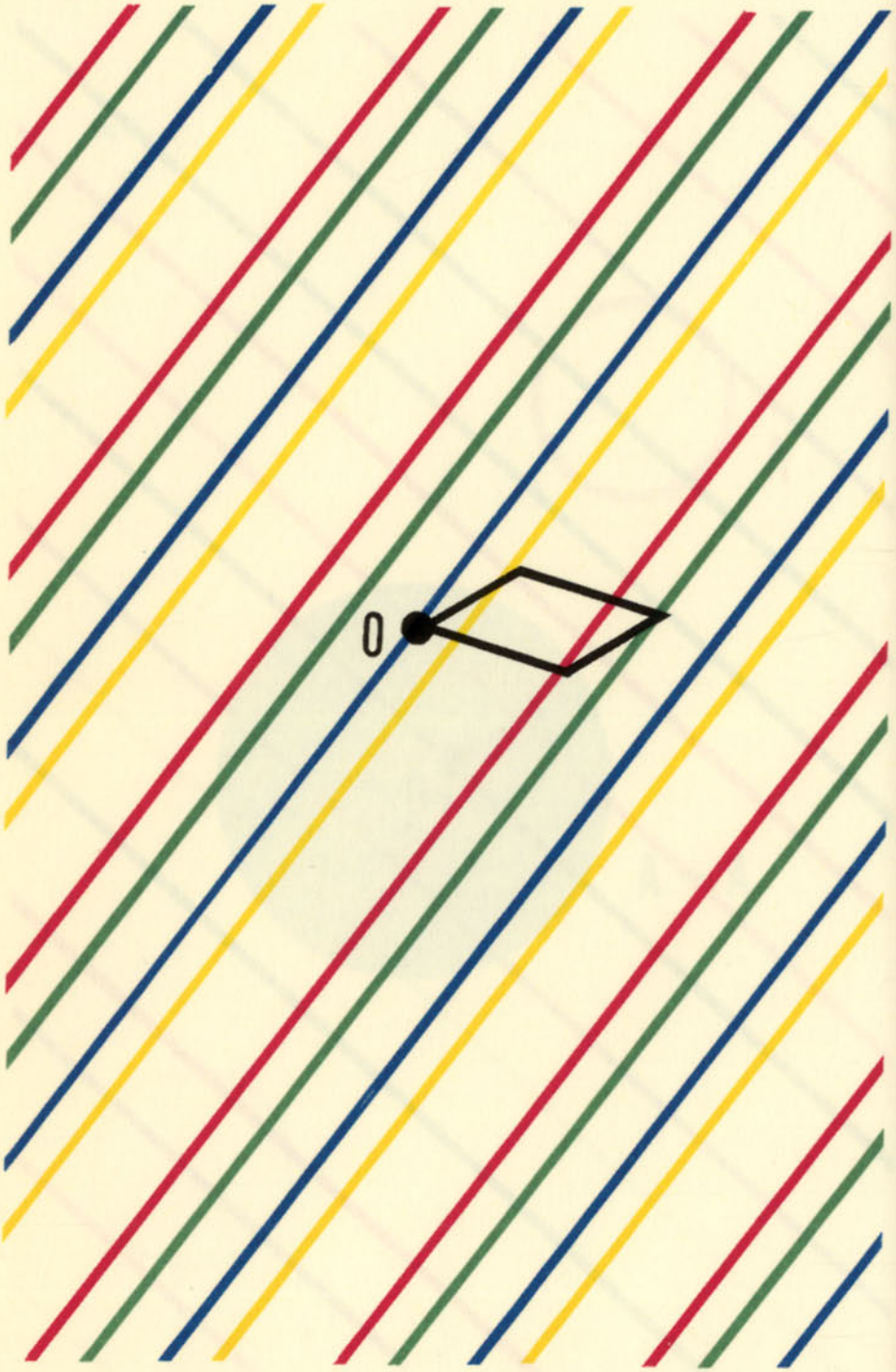


In V, +

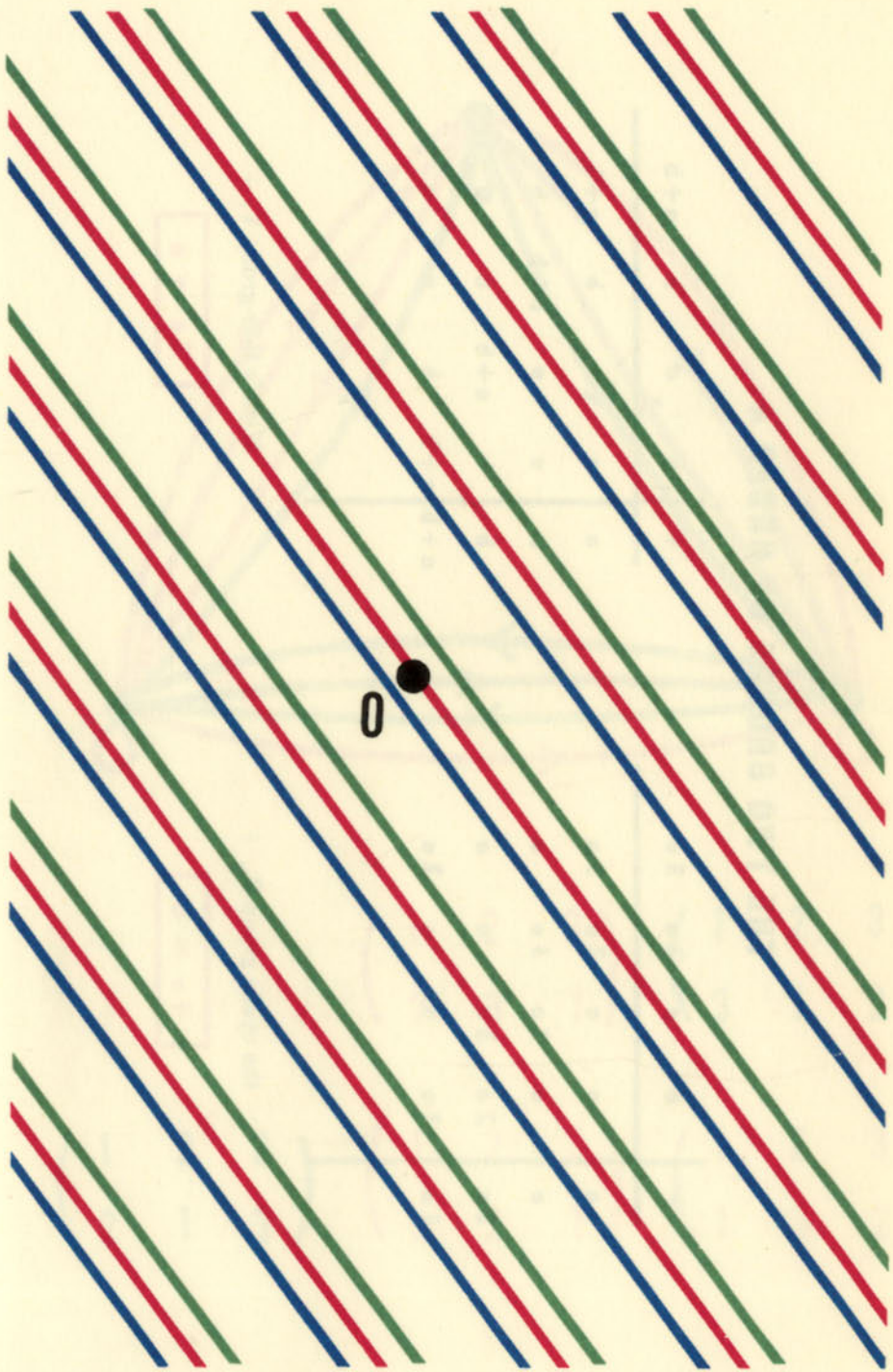




Sixteen elements of V/S



$A, B, A + B \in V / S$



$A \in V/S \qquad -A \in V/S$

THE TWO GROUPS OF ORDER 4

+	o	a	b	a+b
o	o	a	b	a+b
a	a	o	a+b	b
b	b	a+b	o	a
a+b	a+b	b	a	o

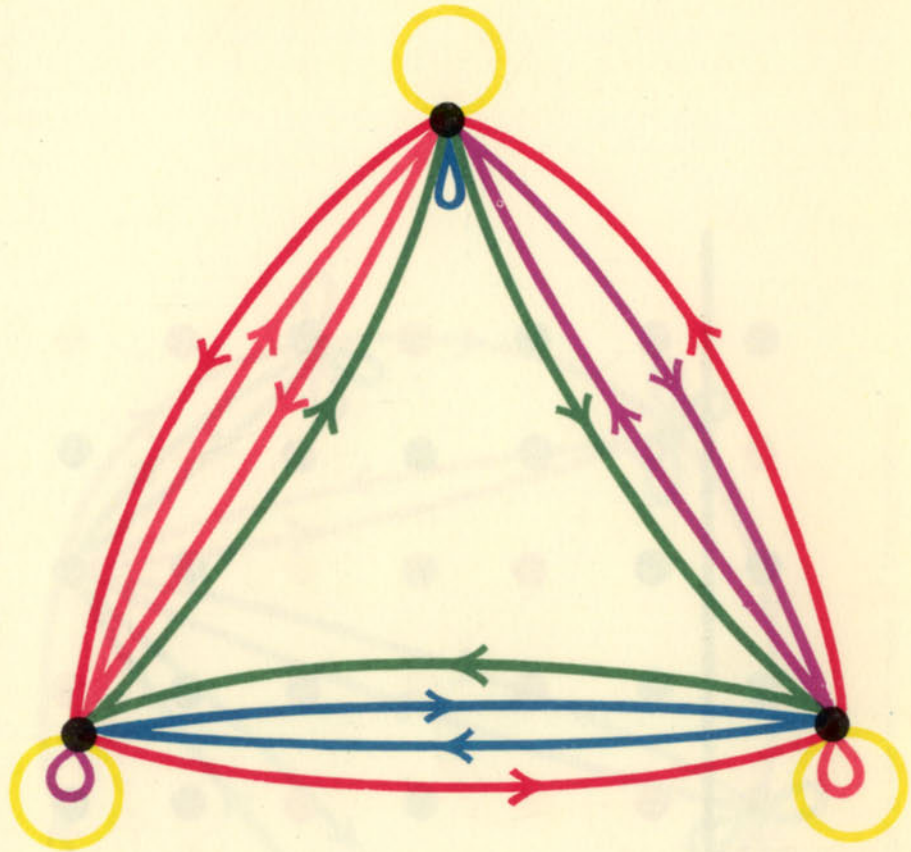
Klein's four-group V, +

$2a = o$

+	o	a	2a	3a
o	o	a	2a	3a
a	a	2a	3a	o
2a	2a	3a	o	a
3a	3a	o	a	2a

the cyclic group Z_4, +

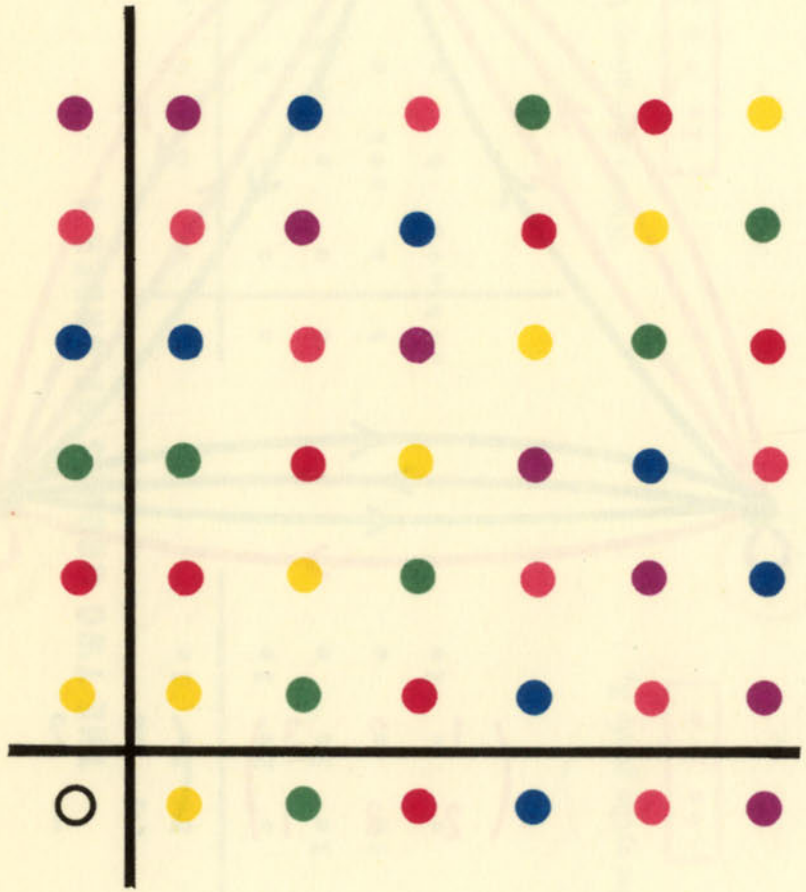
$4a = o$



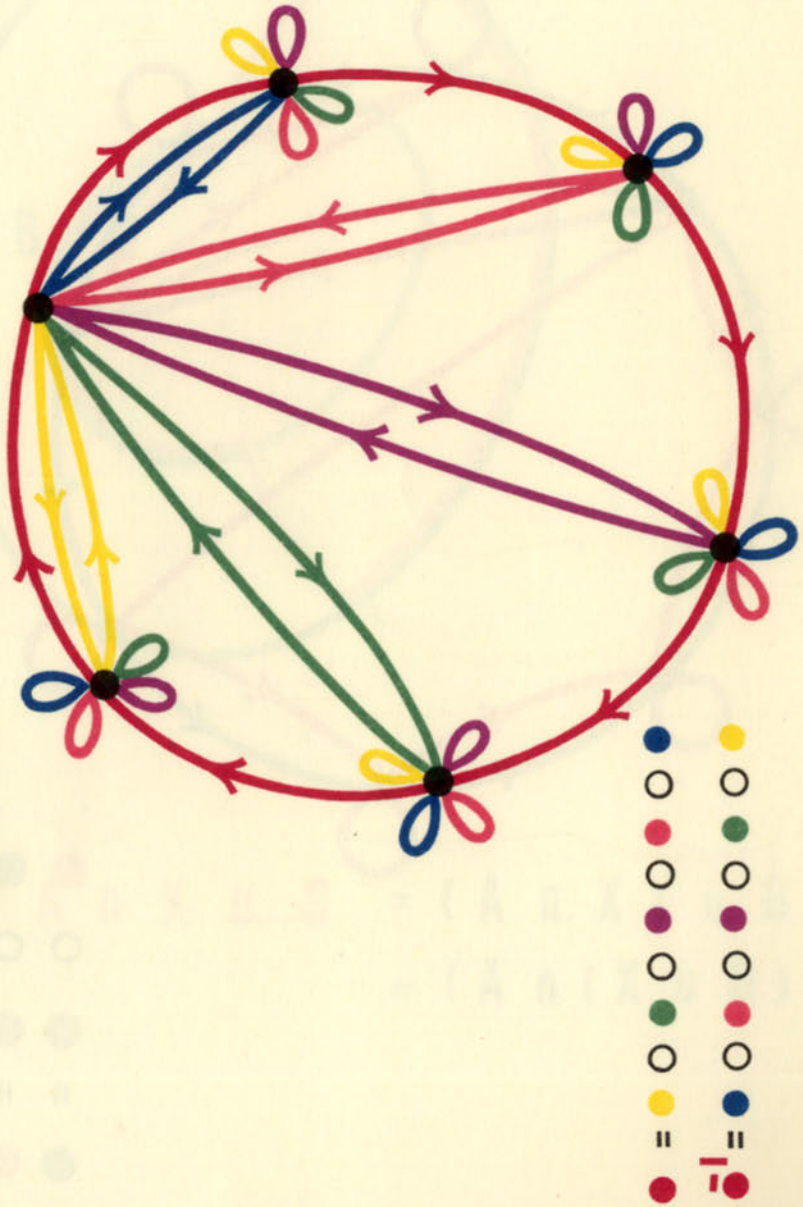
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

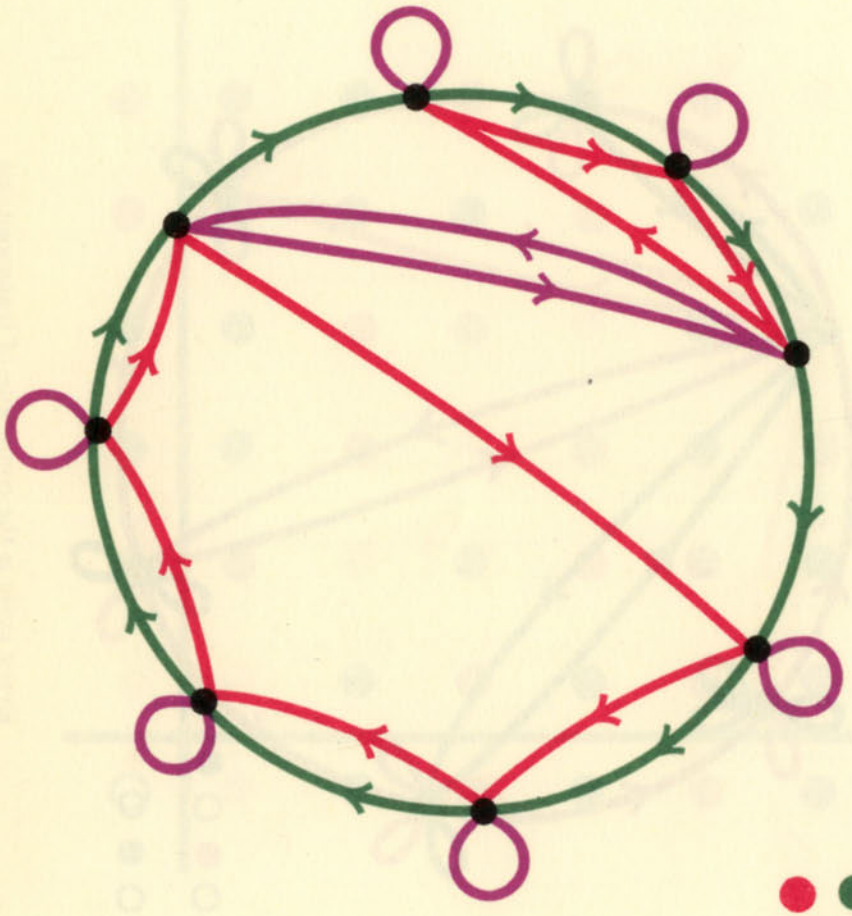
The symmetric group $\mathcal{S}_3$, o

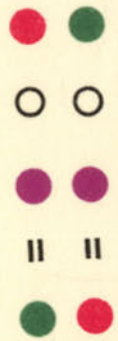


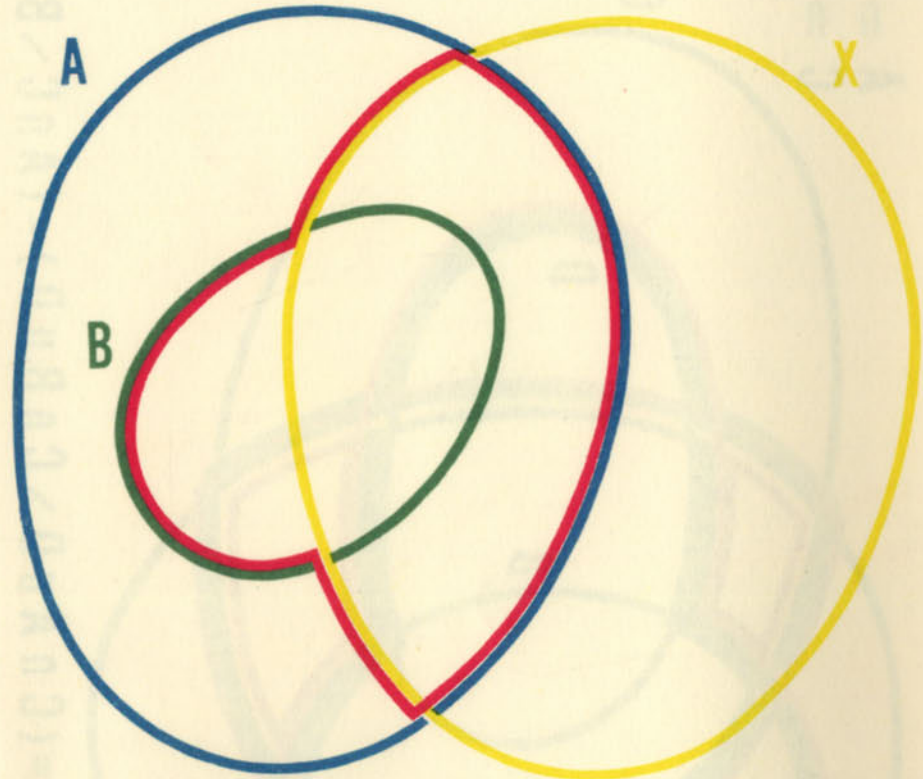
The symmetric group $\mathcal{S}_3$, ∘



Every cycle is the composite of transpositions







$$A \cap X \cup B = (A \cap X) \cup B$$
$$= (A \cap (X \cup B)$$

$$(A \cap C \cup B \setminus A \cap D \cup B) = (C \cap A \cup D \setminus C \cap B \cup D) = (A \cap C \setminus B \cup D)$$

Printed in Great Britain